Forensic Analysis of Android Rooting

Basundhara Dey
PID: ba3661281

Summary: Till date Android is the most popular mobile operating system, used by billions of people. The reason because best smartphones recommended are always Android as it has been featured some of the finest phone hardware available [1]. But to prevent users to gain full access over all sort of facilities, manufactures place over layers of protection over the core system. To access all features over the Operating system, the best answer now a days is "Root". For best example of the current date, people use rooting to skip over the premium pay option of YouTube add skip and play as in background app.
Due to announced legitimacy, Android system can be exploit to vulnerabilities using many one click root method that seems very convenient. But it is just like a 'double-edged sword [2]'. If not controlled carefully, malware author can abuse such exploits to gain unauthorized root privilege.
In this term paper, I have presented three parts, first a detailed analysis of Android root, second part is what will be the pros and cons of rooting a device and lastly I have demonstrated a technical approach for android rooting and discussed the steps. In the end, concluding with my own remarks and list of references that I have used during this term paper.

What is Rooting: If you want to obtain "superuser" privileges to your Android's OS, you need to go for "Rooting". When someone get this kind of permission access, he pursues the ability to load custom software (ROM's), install custom themes, increase performance, increase battery life, and the ability to install software that would otherwise cost extra money (ex: WiFi tethering). You are basically "hacking" your Android device using "rooting". In iOS this feature is same as "Jailbreaking" your phone.
Rooting an Android device benefits two different groups of people. On one end it is interesting for the user itself, because he could get more control over the phone and do tasks with the phone which are not allowed or possible with an unrooted phone. Restrictions on an unrooted phone may occur because the manufacturer does not like the user to do some things or because there are security restrictions. Beside the user also an attacker may be interested in gaining root access. If an attacker could achieve root access he could do whatever he wants on the victims phone without asking permission to do sensible actions or access secret data.

Why it is called 'Rooting': The term "root" is used to describe a user who has

“superuser” rights or permissions to all the files and programs in the software OS (Operating System). The root user, because they have “superuser” privileges, can essentially change or modify any of the software code on the device. You see, your phone manufacturer/carrier only gives you “guest” privileges when you purchase your device. They do this for good reason… they don’t want you getting into certain parts of the software on your phone and screwing it up beyond repair. It makes it much easier for them to manage and update the devices if they lock it all down. This way, all the users are running the same unmodified version of the phone’s software. This makes it much easier for them to support the devices. But, for the tech-savvy crowd, only having “guest” privileges on your device is pretty lame and it locks down a lot of potentially useful features.
Root refers to user gaining access to root directory, ‘/’. This feature is put on by mobile service companies like Verizon, AT&T, Sprint, T-Mobile etc. on smartphones and tablets. This features restricts the user to execute anything on the device as root user. And this concept of “root” use comes from Linux/ UNIX. Having access to root allow the user to execute anything on device even the firmware settings. This privilege also includes listing the active mounted partition on the mobile and user can tweak anything with the system. It can be used to analysis purpose as well. It gives power of a super user, which allows to run any restricted apps and to overclock or under clock the system. So, this process flashes the policies on the previous OS and installs a different operating system. However, it could lead to voiding the warranty or sometimes if done improperly can totally make the phone waste.

Risks of a rooted Smartphone: Root is not for everyone, as the risks can far outweigh the benefits and you are likely to regret your decision once things get messy (and they can get messy). So here is why you should not do it.

- **Expose You to More Security Risks-**
- **Good-Bye to the Warranty-**
- **Cause Update Issues-**
- **Not all devices are created equal-**

Pros of Rooted Android: For the user a rooted smartphone could have lots of advantages and gives him full control over the phone. It is for example possible to customize the look and feel of the user interface, uninstall unwanted applications of the manufacturer or provider which were shipped with the phone or tune the phone for better speed and battery life. There are also applications available, which are just running on a rooted phone. For example automated backup applications, ad blocking applications or applications for using wireless tethering even if not allowed by the telecommunication provider.
A nice and detailed top 10 list of things to do with a rooted phone is described below-

- **Apps Aplenty-**

- **The Latest OS Updates-**
- **Ditching the Skin-**
- **Bloat Banishment-**
- **Speed/Battery Life Boosts-**
- **Extreme Customization-**
- **Infinite Features-**
- **A Free Wi-Fi Hotspot-**
- **Better Backup-**

Key terms Related with rooting: As you learn more about the rooting process, you'll probably run into a bunch of terms that can be confusing. Here are some of the most important ones and what they mean.

- **Root-**
- **ROM-**
- **Stock-**
- **Kernel-**
- **Radio-**
- **Flash-**
- **Brick-**
- **Recovery-**
- **Nandroid-**
- **ADB-**
- **S-OFF-**
- **RUU, SBF, and OPS-**

Classification of Rooting Methods: As noted in the section above, there are two methods to root a smartphone. Both methods are described in detail in the following subsection.

- **Custom ROM Flashing-**
- **Soft Flashing-**

Root an Android Device: So now we get to the good stuff: actually rooting your phone. Unfortunately, every single phone is different, and rooting methods change every time that phone's software updates. With so many Android phones out there, it's become impossible for us to actually list rooting instructions here—especially because we only own a few different phones ourselves.

Luckily, now that you know a thing or two about rooting, you're in a much better position to understand some of the other instructions out there. So, here are a few places you'll find guides, ROMs, and other information about rooting your specific phone.

- **The XDA Developers forums**
- **The Phandroid forums**
- **RootzWiki**
- **The CyanogenMod Wiki**

For the technical part of the paper, I will mention the steps, how to root a One-Plus One Android Smartphone (as I am using the same).

The pre requisite download requirements (set up) are below:

- **ADB USB Drivers -** **http://www.koushikdutta.com/post/universal-adb-driver**
- **Android SDK Slim-** **https://mega.nz/#!ZZdSGaiZ**
- **TWRP-** **http://techerrata.com/browse/twrp2/bacon**
- **Super SU-** **https://download.chainfire.eu/451/SuperSU/UPDATE-SuperSU-v2.01.zip**

- **Ensure the OnePlus One is fully charged**
- **Verify that TWRP recovery is pre-installed on the phone to facilitate rooting**
- **Back up important data and settings on the phone to prevent unexpected data loss during the ROM installation**

Steps to root OnePlus One on Cyanogen OS:

Step 1: Copy the downloaded root zip file to the phone's internal storage and remember the save location

Step 2: Download and install TWRP recovery, and then boot the device into Recovery mode

Step 3: Take a backup of current ROM on your phone: choose Backup and then do a 'Swipe to BackUp' gesture from the bottom of the screen.

Step 4: Wait until the backup completes and then go ahead with the root installation steps as outlined below:

Step 5: Return to the main menu of TWRP recovery and hit Install. Go to the folder where you saved your root zip file and select it. Then perform the action 'Swipe to Confirm Flash' from the bottom of the screen.

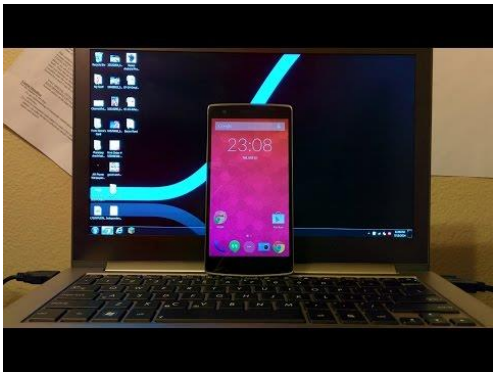
Step 6: Wait until the root is completely flashed on your phone and then return to recovery's main menu, choose Reboot > System

Step 7: Navigate to Settings > About Phone and then tap the build number 7 times to unlock developer options

Step 8: Return to the main Settings menu, select developer options and then tick the Root Access checkbox to enable root for apps as well as in ADB

Step 9: Finally, launch SuperSU app > choose Settings and then uncheck the Respect CM root setting option.

For the video part, I have just purchased my phone few months back, so I am unable to take a video in this moment. As rooting diminish the warranty, so I cannot take chances with this new one. Here, I am providing a reference link [12] [13] that I can use the time to root my phone. This steps are exactly the same that I have to follow while rooting my device.



Things you can try after rooting your device: Now you have just Rooted your Android device, and looking for things you need to do just after you Root Your Android Smartphone [14]. Just to note, Rooting is fun, but also pretty risky, so we don't encourage it. Performing the hack might brick your smartphone or tablet, and then your warranty won't cover the damage. Root only at your own risk!

- **Check Root-**
- **Install CWM-**
- **Flash Custom ROMs-**
- **Increase RAM of Android Device-**
- **Increase Internal Memory-**
- **Overclocking-**

Further research: Came across an excellent tool ORBOT, which is a part of TOR project since it uses Onion routing and it works in android devices. This works well with Orweb web browser which integrates with Orbot easily. Orbot provides a local HTTP proxy and the standard SOCKS4A/SOCKS5 proxy interfaces into the Tor network. But to install the Orweb, the user needs root permissions on the device.
Here we notice that one mechanism for anonymity is causing the device to compromise on security by rooting the device. Once the device is rooted, and hacked, the hacker can literally do anything with the device.
Considering hacker is successful pursuing the above tasks. Does that mean, we cannot get hold of the hacker? However, as per research it has been found that the hacker is still identifiable.

To pursue this experiment, following are the requirements:

- **One Plus One smartphone running Android OS**
- **Orweb v2.28 Android app**
- **Titanium Backup v5.5.2.1 Android app**
- **Odin3 and S2 Root software for rooting the smartphone**
- **SQLite Database Browser v1.2**
- **Root Explorer v2.19, to be installed on the smartphone**
- **CF-Root kernel, to be installed on the smartphone**
- **Micro USB cable to connect the forensics workstation to the smartphone**
- **Laptop PC running Windows XP SP3 as the forensics workstation**

Analyzing the result in the rooted device about the usage detail or performing forensic on the smart phone is as follows:

In order to perform a logical acquisition through the Titanium Backup utility or to access the contents of the Orweb browser database in a live examination, it was necessary to root the device. We were able to access the Orweb browser's application files (located in "/data/data/info.guardianproject.browser" both through examining the backup on the forensic workstation, and through the Root Explorer app on the Android device. Using the SQLite Database Viewer, we were able to examine the contents of these files and find some traces of the web browsing activity under investigation.
The analysis of each of the analyzed files is as:

- **Forensics expert can see the history of the visited files stored in the database webview.db.**
- **The history to which the user chatted before is also stored in webview.db/formdata.**
- **Logged in information and other Bluetooth transfer information is also logged into webview.db file.**

This clearly proves that if the smart phone is rooted and if the user uses anonymity software to hide its identity. Then, it's still possible to retrieve enough information from the device to keep track of its logs and other important features.

Conclusion: The concept of rooting and anonymity is connected to each other on several points including getting to know the usage pattern of any smart phone.
Initially, there was discussion on how the hacking of smart phone is very important to get to know the activity of the user, which was showing using google knowing person's movement and another one regarding a tool that you can access from anywhere in the world to control android smartphone.
Finally, we found that in case, the hacker use anonymous software after wards, how easy it is to get the information that what stuff or action was performed in the absence of the genuine user, given the condition the device is rooted.

References

[1] Best Smartphones
http://www.usatoday.com/story/tech/2015/10/24/best-smartphones-under-500/74394566/

[2] Zhang, Hang, Dongdong She, and Zhiyun Qian. "Android Root and its Providers: A Double-Edged Sword." *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015.

[3] Think twice about android root
http://www.sciencedaily.com/releases/2015/10/151013175904.htm

[4] Android Developers. October 2, 2013. Accessed on October 10, 2013
https://developer.android.com/about/dashboards/index.html

[5] 10 reasons to root your Android device
https://www.androidpit.com/10-reasons-to-root-your-android-device

[6] Shao, Yuru, Xiapu Luo, and Chenxiong Qian. "Rootguard: Protecting rooted android phones." Computer 47.6 (2014): 32-40.

[7] Jang, Won-Jun, et al. "Rooting attack detection method on the Android-based smart phone." Computer Science and Network Technology (ICCSNT), 2011 International Conference on. Vol. 1. IEEE, 2011.

[8] Al Barghouthy, Nedaa, Andrew Marrington, and Ibrahim Baggili. "The forensic investigation of android private browsing sessions using orweb." Computer Science and Information Technology (CSIT), 2013 5th International Conference on. IEEE, 2013.

[9] 5 reasons not to root your Android device
https://www.androidpit.com/5-reasons-not-to-root-your-device

[10] What is Rooting on Android? The Advantages and Disadvantages
http://droidlessons.com/what-is-rooting-on-android-the-advantages-and-disadvantages/

[11] CamStudio-
http://camstudio.org

[12] YouTube video
https://www.youtube.com/watch?v=x7C9Rmk2RxQ

[13] [GUIDE] OnePlus One - How to Unlock Bootloader, Install Custom Recovery and Root
http://forum.xda-developers.com/showthread.php?t=2788632

[14] 30 Must-Try Apps for Rooted Android Phones
http://www.hongkiat.com/blog/popular-apps-for-rooted-android/