COMSEC 2 Project Documentation

Topic: Exploiting Android Operating System through Rooting

Vulnerability Type: Mobile

Elijah Angelo Alcarde

Daniel Tagala

Rainiel Cerveza

Tom Tonoike

December 18, 2015

Abstract

The project will focus on rooting Asus Zenfone 5 with operating system Android 4.4.2(Kitkat). Rooting an android phone allows the user to have more control over its features. Different apps that are only compatible on rooted phones are available from the XDA forums and they will be used to modify different features of the sample phone. Some of the adjustments could also be done manually.

Behind these advantages however, also come some disadvantages. Rooting gives a user or an app too much control over a phone and this can cause damage whether unintentionally, faulty installation of an app, or intentionally, malicious apps and software installed in the phone. The project will try to look into these disadvantages and try to assess whether rooting is worth its risks.

Background of the Study

Usually, users feel unpleasant whenever they see an Android phone full of pre-installed bloatware and ads that ultimately slows down the phone itself. An exploit in Android phones exists just for that purpose – it's called 'Rooting an Android Phone'. Basically, users will have administrator access that has control all over a phone's inner firmware. Although it may be considered as a vulnerability, it also proves that gaining such capabilities for a mobile device could also be beneficial.

Things such as: unlocking hidden features, changing CPU clock speed, boosting your phone's speed and battery life. Moreover, one can remove any ads in any app; which is one of the more common problem for Android users. For socially inept persons, you can tweak or remove your pre-installed firmwares and automate everything.

Objectives

- Introduce rooting to people – in initiating the project, the group will share the benefits and impacts of having one's Android phone being rooted. It will help them in understanding the pros and cons of doing such method to his mobile device.
- Reduce the risk – rooting a phone gives an overall access to its inner firmware. It simply means that one can block ads where most viruses came from. One could also back up data in an easier and convenient manner; which helps users secure their data.

- No more restriction – one can only imagine the possibilities of having root access to their phones. With the concept of ‘internet of all things,’ daily tasks could be done in a more efficient process.

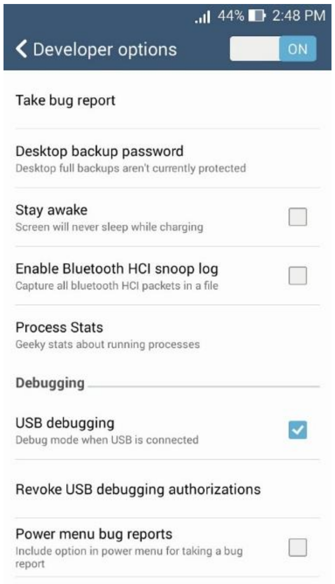
Methodology

Tools needed to setup rooting:

- Root z5 kitkat v2
- Intel Android Device USB driver
- Micro USB cable
- Windows pc

1. Download and install Intel Android Device USB driver.

2. Connect phone to pc using micro USB cable, and enable USB debugging mode from settings>developer options.



44% 2:48 PM

Developer options ON

Take bug report

Desktop backup password
Desktop full backups aren't currently protected

Stay awake ☐
Screen will never sleep while charging

Enable Bluetooth HCI snoop log ☐
Capture all bluetooth HCI packets in a file

Process Stats
Geeky stats about running processes

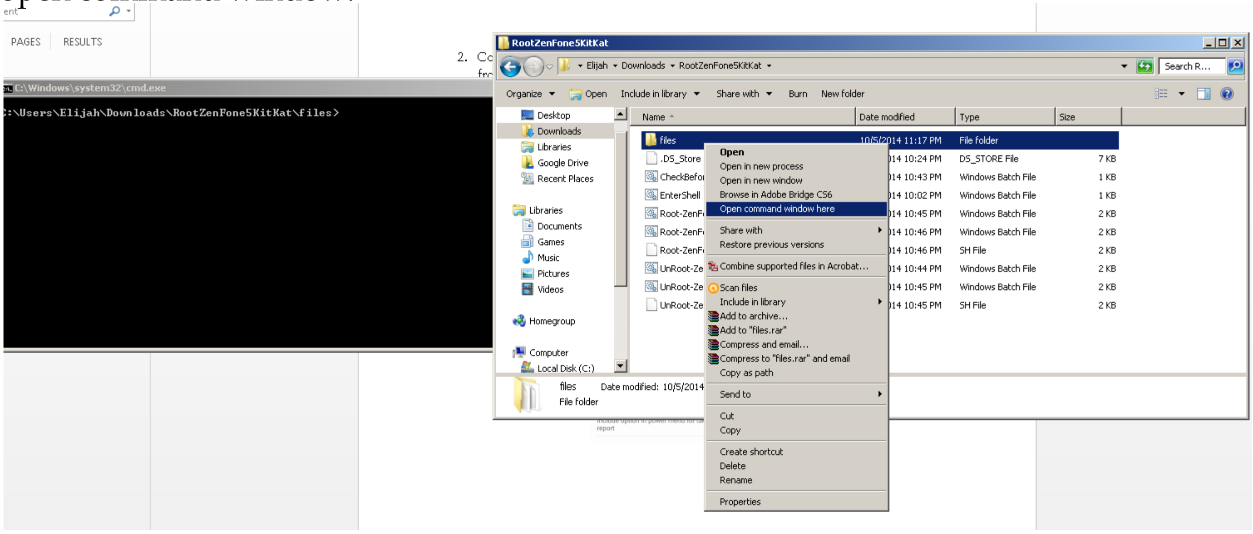
Debugging

USB debugging ☑
Debug mode when USB is connected

Revoke USB debugging authorizations

Power menu bug reports ☐
Include option in power menu for taking a bug report

3. Extract the downloaded Root z5 kitkat v2, and click files>hold shift + right click to open command window.

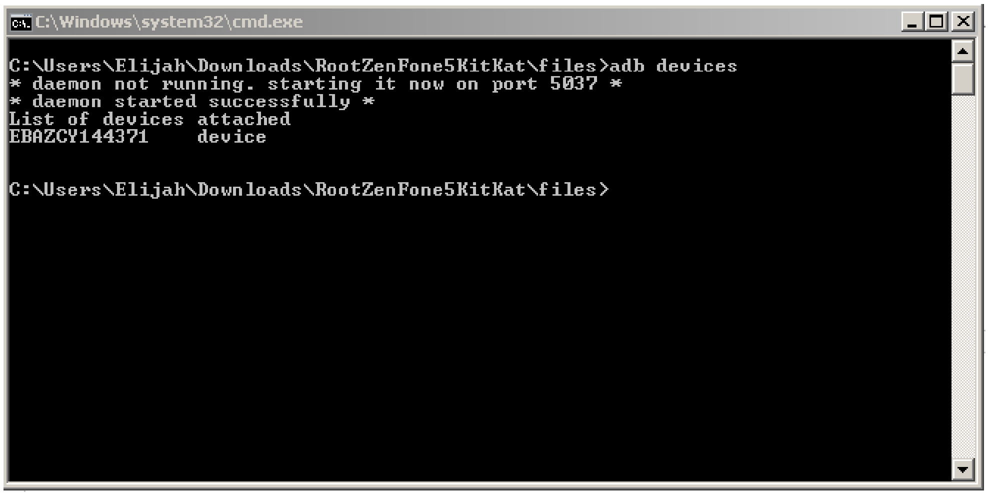


```
:\Users\Elijah\Downloads\RootZenFone5KitKat\files>
```

Name	Date modified	Type	Size
files	10/5/2014 11:17 PM	File folder	
.DS_Store	014 10:24 PM	DS_STORE File	7 KB
CheckBefo	014 10:43 PM	Windows Batch File	1 KB
EnterShell	014 10:02 PM	Windows Batch File	1 KB
Root-ZenF	014 10:45 PM	Windows Batch File	2 KB
Root-ZenF	014 10:46 PM	Windows Batch File	2 KB
Root-ZenF	014 10:46 PM	SH File	2 KB
UnRoot-Ze	014 10:44 PM	Windows Batch File	2 KB
UnRoot-Ze	014 10:45 PM	Windows Batch File	2 KB
UnRoot-Ze	014 10:45 PM	SH File	2 KB

files Date modified: 10/5/2014
File folder

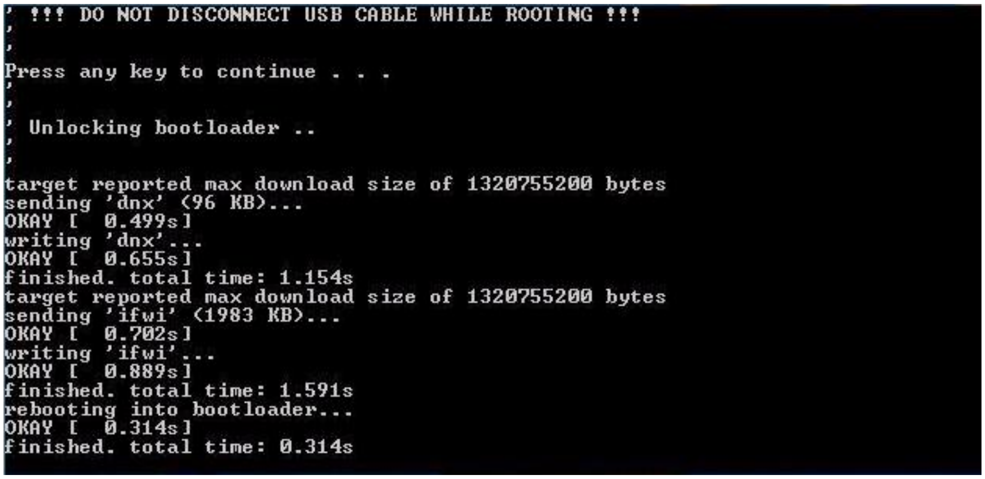
4. Type "adb devices" and press enter, the phone's serial number must appear to proceed.



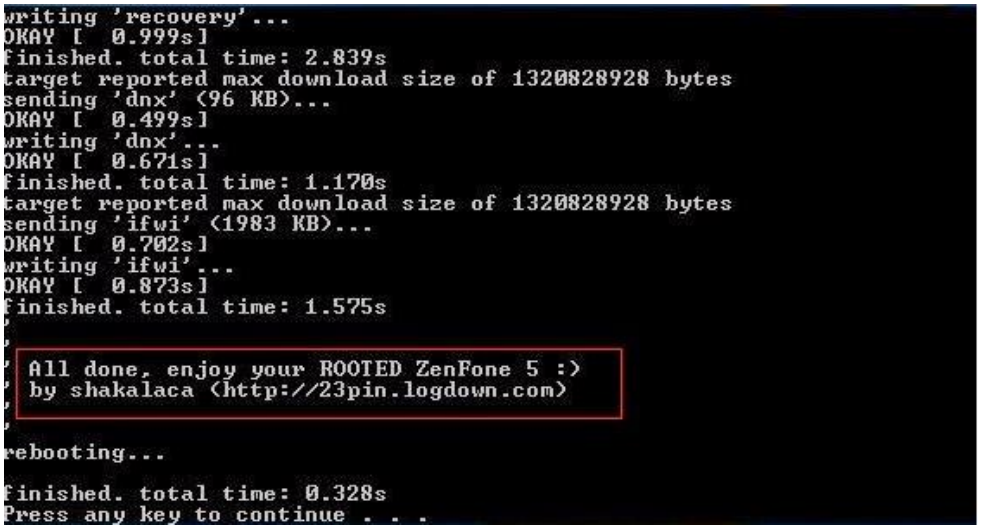
```
C:\Users\Elijah\Downloads\RootZenFone5KitKat\files>adb devices
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
List of devices attached
EBAZCY144371    device


C:\Users\Elijah\Downloads\RootZenFone5KitKat\files>
```

5. If the word "unauthorized" appeared instead of "device," reconnect phone from pc – check "always allow from this computer."
6. Double click Root-ZenFone5-en in the RootZenFone5KitKat folder to start the script in rooting. The phone will reboot several times during the procedure.



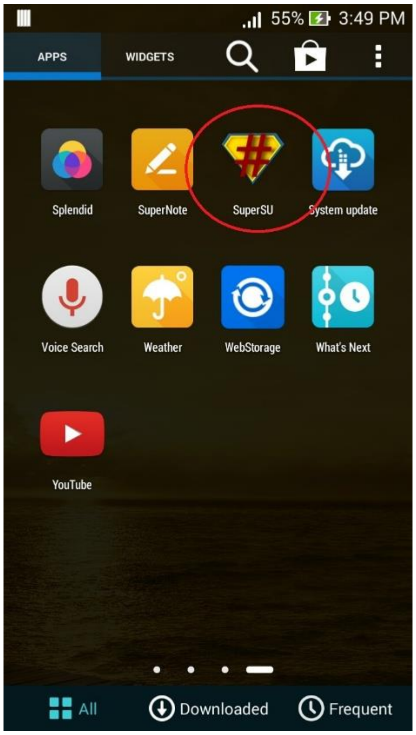
```
' !!! DO NOT DISCONNECT USB CABLE WHILE ROOTING !!!
'
'
Press any key to continue . . .
'
'
' Unlocking bootloader ..
'
'
target reported max download size of 1320755200 bytes
sending 'dnx' (96 KB)...
OKAY [  0.499s]
writing 'dnx'...
OKAY [  0.655s]
finished. total time: 1.154s
target reported max download size of 1320755200 bytes
sending 'ifwi' (1983 KB)...
OKAY [  0.702s]
writing 'ifwi'...
OKAY [  0.889s]
finished. total time: 1.591s
rebooting into bootloader...
OKAY [  0.314s]
finished. total time: 0.314s
```



```
writing 'recovery'...
OKAY [  0.999s]
finished. total time: 2.839s
target reported max download size of 1320828928 bytes
sending 'dnx' (96 KB)...
OKAY [  0.499s]
writing 'dnx'...
OKAY [  0.671s]
finished. total time: 1.170s
target reported max download size of 1320828928 bytes
sending 'ifwi' (1983 KB)...
OKAY [  0.702s]
writing 'ifwi'...
OKAY [  0.873s]
finished. total time: 1.575s
'
'
' All done, enjoy your ROOTED ZenFone 5 :)
' by shakalaca (http://23pin.logdown.com)
'
'
rebooting...

finished. total time: 0.328s
Press any key to continue . . .
```

7. Check phone apps, the rooting is a success if one can see SuperSU.



To unroot the device, run the unroot script from the downloaded folder; or tap "full unroot" in SuperSU.

Useful apps that could be installed after rooting the phone:

- Device Control – *"Tweak all kinds of settings with this app including CPU and GPU frequencies, vibration strength, screen color temperature, voltage control, and kernel specific extras. There's even an automation feature, app management support, and editors for system configuration files all built-in. As long as you know what you're doing this is a potentially powerful app."*
- System Tuner – *"Analyze exactly what is going on with your Android device and make a few tweaks to tune up performance with this free app. It enables you to tweak CPU settings, kill background processes and apps, backup and restore apps and their settings, tweak cache and memory settings, and a whole lot more. You can dig into exactly how your device is running, but exercise some caution before you start making changes."*

Conclusion

Risk Analysis

Rooting an android phone brings many advantages, however, it also opens up the phone to different risks while and after rooting the phone. The first risk to consider is the phone turning to a brick because of wrong rooting procedures. The term brick is used when the software of phones and other devices gets damaged that it becomes useless. Sometimes there are ways to recover the phone, however there are also times that the damage is permanent. Another risk is that rooting a phone instantly voids its warranty. This means that even if the phone has defects from manufacturing, the owner could not return the phone to the seller to be changed for a new one. The third risk of rooting a phone is that rooting opens the phone to a whole new set of malwares. Rooting provides apps more privileges so that a user can customize it more. Having more privileges however, the phone is more open to malicious apps.

Solution

Do not let your Android Operating System be outdated for a very long time, upgrade to the latest version – Marshmallow 6.0. Although there are reviews that which says that there are still bugs, chances are, rooting it will nearly be impossible as of today. If the device is incompatible to the latest Android OS, at least update it to the highest version which is compatible to the device.

Recommendation

- Update system to Android 4.4.3 or greater.
- Developers should create a patch where it blocks the user from rooting their phone or limit the access in phone settings as developer mode.
- New version updates must reach the user's expectation. In that case, most users will avoid rooting their phone since what they need is already available.
- Mobile developers should include the things which is available when your phone is rooted to non-rooted phone. E.g. uninstalling basic software, killing running apps, etc.
- In the end, the user has the discretion to root his phone.

Sources:
http://forum.xda-developers.com/android/general/root-asus-zenfone-5-kitkat-4-4-2-100-t2947092

http://www.digitaltrends.com/mobile/best-android-root-apps/