ARL-TN-0706 ● SEP 2015


US Army Research Laboratory

# Rooting an Android Device

by Ken F Yu

Approved for public release; distribution unlimited.

## NOTICES

### Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-TN-0706 ● SEP 2015

US Army Research Laboratory

# Rooting an Android Device

**by Ken F Yu**
*Computational and Information Sciences Directorate, ARL*

**Approved for public release; distribution unlimited.**

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED (From - To) |
|---|---|---|
| Sep 2015 | Final | 4/1/2014–9/1/2014 |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| Rooting an Android Device | W911QX-14-F-0020 |
| | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |

| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
|---|---|
| Ken F Yu | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| US Army Research Laboratory<br>ATTN: RDRL-CIN-D<br>2800 Powder Mill Road<br>Adelphi, MD 20783-1138 | ARL-TN-0706 |

| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
|---|---|
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

Approved for public release; distribution unlimited.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

This document provides a step-by-step guide on how to root an Android device, which allows the user to have “superuser” capability with the device.

**15. SUBJECT TERMS**

ELIDe, Android, pcap

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Ken F Yu |
| Unclassified | Unclassified | Unclassified | UU | 12 | 19b. TELEPHONE NUMBER (Include area code)<br>(301) 394-3181 |

**Standard Form 298 (Rev. 8/98)**
**Prescribed by ANSI Std. Z39.18**

## Contents

INTENTIONALLY LEFT BLANK

## 1. Overview

The purpose of this document is to demonstrate how to gain administrative privileges on an Android device. The term "rooting" is defined as a process of gaining administrative commands and functions of an operating system (OS). In order to monitor live network traffic on any Linux-based or, in this case, Android system, it is necessary to have administrative rights to gain access to any of the hardware devices, such as the Wi-Fi connection.

## 2. Configurations Used

The following is a list of software and hardware used for development and testing:

- Operating System: Red Hat Enterprise Linux, version 6.5
- Android Development Tools (ADT), version 22.3.0-887826
- Saferoot[1]
- Samsung Galaxy S3
- Dell Precision T7400
  - 8-GB Memory
  - Intel Xeon X5472 Central Processing Unit (CPU)
    - 64-bit quad and dual-core
    - 3.0 GHz

## 3. Rooting Android Devices

The rooting method used for the Samsung Galaxy S3 is called Saferoot[1]—a well-known, open- source software. According to the Saferoot website, the process of rooting the device may void the manufacturer's warranty; therefore, use this feature at your own risk. Because any manufacturer can have its own modified version of an Android OS, there is no guarantee that the Saferoot method will work with all Android devices. Moreover, this Saferoot rooting method is applicable for the Samsung Galaxy S3 as well as many other Android devices, but there are several steps involved in rooting an Android device (as shown on the next page). Most of these steps will be the same for all Android devices.

## 3.1 Step 1—Set Up Android ADT

Download the Android Software Development Kit (SDK).[2] Install the ADT from the SDK.

## 3.2 Step 2—Set Up USB Driver on Host Computer

Before any communication between the host and Android device can be established, the host computer must have the ability to "access" the Android device. Fortunately, the Red Hat-based system already has a built-in USB driver to access the Samsung device. For other OS host computers, the USB driver may have to be downloaded from the manufacturer's support site. Once the USB driver is installed, the OS should be able to recognize the device. When the connection between the host client and the Android device is made, use Android Debugging Bridge (adb) by typing "adb devices" and it should list the device as part of the connected list.

## 3.3 Step 3—Enable Android Debugging

Before an Android device can be used for rooting, the debugging mode must be turned on. To enable this feature on an Android device, go to "Settings" and then "About Phone" or "About tablet". Find "Build Number", then tab on the "Build Number" 7 times or until develop mode is enabled. Once the developer option is visible, make sure the "USB Debugging" mode is checked.

## 3.4 Step 4—Get Saferoot

Download the Saferoot[1] package. Unzip the archived file.

## 3.5 Step 5—Rooting Android

The Saferoot package should contain scripts for installing tools that grant root privileges for both Windows and Linux. For the Linux system, open a shell window and use "cd" command to change the directory where the Saferoot files are. Type the "sh ./install.sh" command, and the install script will ask for installation of BusyBox.[3] BusyBox is an open-source program that provides another set of Linux shell utilities, which the average Unix user would expect to see on a typical Unix/Linux system. If the shell (terminal emulator or adb shell) is not needed, then you may not want to install BusyBox; however, it is advisable to install BusyBox. SuperSU is part of the BusyBox installation:

- If SuperSU asks you to update the su binary, choose the "Normal" method.
- If SuperSU asks you to disable KNOX, allow it.

This method will not set the KNOX warranty-void flag, according to the author of Saferoot. However, it will set the “Custom” flag, which should not affect phone operation.

Ensure that the phone or tablet is on and active while the rooting process is underway, and monitor the Android device and host computer for progress of the script to determine whether the installation succeeded or failed. Do not unplug the phone unless prompted by the rooting script. Be sure to leave the device connected to the host until the process has been completed. If the device is successfully rooted, the “su” utility should be installed and allow root access to the device using “adb”. To verify whether the device was properly rooted, type “adb shell” on the host client, then the “$” prompt should appear. Type the “su” command, and the prompt should change to “#” to show that root access has been granted.

## 4. Conclusion

This document serves as a tutorial on how to grant user administrative privilege to an Android device by employing the rooting method. Once it is rooted, the device will allow the user to freely access and manipulate all software within the device. Caution must be taken when employing this method.

## 5. Notes


1. Saferoot: Root for VRUEMJ7, MK2, and Android 4.3. [accessed 2014 Dec 04] http://forum.xda-developers.com/showthread.php?t=2565758.
2. Get the Android SDK. [accessed 2014 Dec 04] http://developer.android.com/sdk/index.html.
3. BusyBox. [accessed 2014 Dec 04] http://www.busybox.net.

1 DEFENSE TECHNICAL
(PDF) INFORMATION CTR
DTIC OCA

2 DIRECTOR
(PDF) US ARMY RSRCH LAB
RDRL CIO LL
RDRL IMAL HRA RECORDS MGMT

1 DIRECTOR
(PDF) US ARMY RSRCH LAB
RDRLCIN D
K YU

INTENTIONALLY LEFT BLANK