



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

Project DeGoogled Android OS

Harish Kumar H C¹, Aayush Neupane², Bibek Prasad Yadav³, Dhiraj Kumar Mandal⁴,
Mahaboob Alam Momin⁵

Assistant Professor, Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology,
Bangalore, India¹

Students, Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology,
Bangalore, India^{2,3,4,5}

ABSTRACT: Google Services are used by almost every smartphone and this has been contributing to Google's empire of advertisement to be over 200 billion dollars. The major source of their advertisement viewers come from the android users from all over the world. Google wants to display advertisements in their user's screen of products and services in which they are interested. For this, Google tracks down the data, and activity of their users to determine what advertisement to display. This ever-growing presence of surveillance giants creates a huge security concern and now its time to do something about it. This article talks about how de googled Operating System (OS) can help us solve the issue of data being acquired by google and we can prevent it from monitoring it.

KEYWORDS: GSM(Google Mobile Services); Android Open Source Project(AOSP); advertisement(ads); stock ROM; OS(Operating System); micro-G service; vendor; device tree; bootloader; kernel; Open Handset Alliance(OHA)

I. INTRODUCTION

Android has become a household gadget for people around the world. The world has become dependent on the android system for daily commute to communication, entertainment to payment, information to the internet, and the android comes into the picture. Its robustness and the ability to run smoothly even in lower end devices make it a very powerful tool to have reached up to billions of user's bases. But the problem lies when the data is continuously shared over the android and Google intervenes with the data. Google is a must have feature in the androids, because almost all features are provided and ruled by the google. Google makes hundreds of billions in dollars per year only from the ads, excluding every service (neat from the ads). So google tries to study the behavior of the users more and more and access more and more data from the users to know their psychological patterns, preferences and interests and send the data to the ad agencies to use it for the company ads. And this is where the security concern arises.

The Android Operating System is a free and open source, fully customizable mobile Operating System platform. Android Open Source Project(AOSP), which provides a framework for the development of Android, uses a community-driven model for the improvement of mobile Operating System platforms. AOSP is led by Google and the Open Handset Alliance(OHA). Android source code is released under an open source and proprietary firmware, especially the firmware required for accessing Google Play Services. Google Play Services, generally referred to as Google Mobile Services (GMS), has system-level control over the mobile device. It is part of the Google Apps package and is proprietary.

Here comes the deGoogled OS into picture. A deGoogled Operating System is a system based on the android, but all the Google mobile services are eliminated. A deGoogled OS has the clean android, on top of which minimalistic apps are provided like phone, contacts, messages, camera, bing or duckduckgo powered browser, gallery and files. All the other bloatwares and Google Apps that come preinstalled with the versions of android OS are eliminated. In this way, we can secure our data and be safe from Google and Ad agency Surveillance.

II. EXISTING SYSTEM

Currently the android operating system is composed of android kernel at the bottom, and the android OS above it. Above the android, companies provide their own UIs and OS versions like ONE UI, MIUI, OXYGEN OS, HIOS etc.

Above these OSes, GMS (Google Mobile Services) exist and on top of it all the applications are running. Therefore, all the data related are also above the GMS which makes Google to easily scrap our data. Android is the most used operating system in today’s world with more than 2.7 billion active users, being 75% of total mobile phone market. But the major problem is with the Google mobile services running on each and every phone today that exist in this world, collecting huge amounts of data from the users device and selling it to the advertising agencies and many such companies. A very famous quote “Privacy is a myth in tech world”, all thanks to services like google who collect data like place visited, search results, WiFi password, UPI pin, Close relatives number, bank details, credit/debit card details, personal documents, to whom we talk, messages, call recordings, gallery, mail, documents, music, videos and lot more stuff in order to understand person's interest, making search results more better and better. Which will also help them in marketing or making content reach a large audience ultimately to increase profits and companies growth.

Currently the Government of India is working on BharOS, which is also Google services free system based on the linux kernel, promising more security and flexibility. China, is already making use of Google free Operating system named Harmony OS, also based on android kernel.

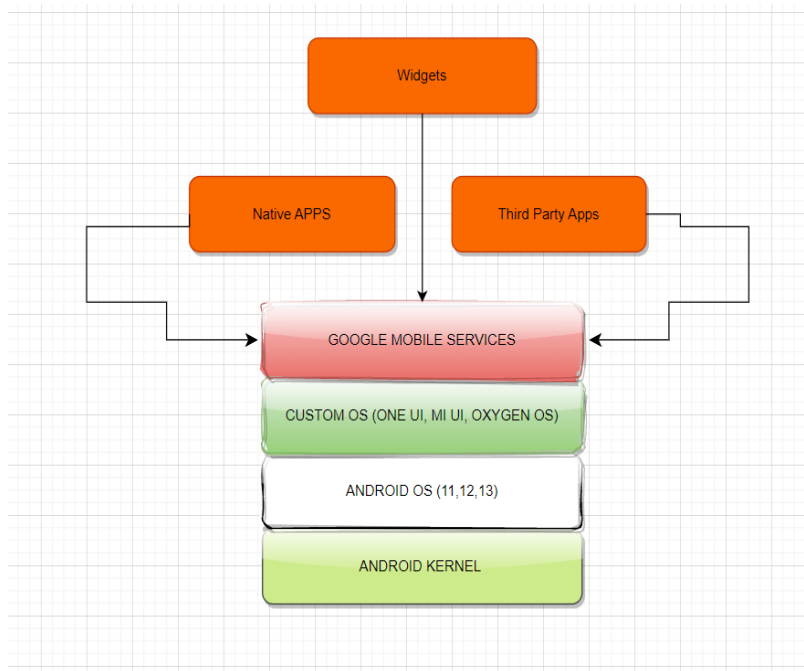


Fig. 1: Existing System

III. PROPOSED SYSTEM

With the ever-growing surveillance presence of advertisement giants like Google(Alphabet) and Meta(Facebook) on your personal devices (including smartphones), it is time to do something about it. One of the most effective ways to do that is by installing a privacy/security-focused Android ROM. A de-googled phone means stripping away unnecessary software and other things that aren’t necessary for the user. Usually the android phones have their UI binded with the Google Mobile Services, a bundle of applications and services that assure our phones to be multi functional and to provide support for certain applications, but they do come at the cost of Privacy. In the proposed system, the central idea is to remove the google services from the UI bundle and provide a clean custom UI above the android OS (AOSP). While this does mean fewer apps and games installed, it also means that the phone would run faster. Another benefit is that it removes potential security threats that can cause harm to the device.

ADVANTAGES OF PROPOSED SYSTEM

- With tethered mobile devices, the phone's VPN or Tor can be used.
- Datura FireWall gives you access control for all of your applications.
- microG is a replacement for some functions of Google Play Service while maintaining much more anonymity
- It makes sure that the operating system hasn't tampered with Verified Boot
- Using OpenPGP (Pretty Good Privacy) encryption, email clients like Thunderbird and K-9 Mail can open emails from users who use PGP (Pretty Good Privacy), which lets them verify both the sender's identity and their own signature.

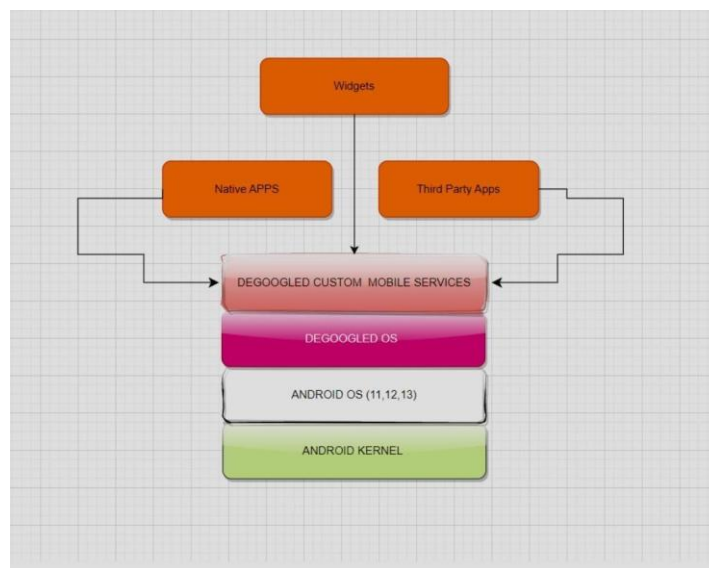


Fig. 2: Proposed System

IV. RELATED WORK

Shreyas S. [1] has an exchanged view on Custom ROM which is a standalone variant of Android that includes Kernel, apps, and all other services that are required to run the device. From the paper, drawbacks concluded are Battery Life Problems, Hardware Issues, Bugs. Muhammad Suleman, Xiaojian Zhong, Yuxia Sun [2] have deliberated about the comparison of stock ROMs and custom ROMs in terms of size, boot time, memory usage and performance. Multiple ROM features are analyzed in the comparison. An Android app was developed that facilitates the users in installing ROMs for devices. However in stock ROMs several services are running in the background all the time that degrades the system performance. 15 custom distributions were used for the Note 3, but due to limited space. Meet Kumar, Rajendra Kumar Parekh [3] talks about the device's firmware and by default comes with a pre-installed ROM on the device known as "stock ROM". These stock ROMs come with a lot of restrictions, fewer features, and less customizability. If the user does not follow the procedures correctly, the device may be bricked and rendered inoperable. Rajashekhar Ponakala [4] has deliberated about the following terms: MicroG Project which is a re implementation of Google Services and libraries., Service Core (GMS Core) that runs functionality like Google Play Services or Google Maps API, Service Framework Proxy (GsfProxy) which uses Google Cloud Messaging Services with Gsm Core, Unified Network Location Provider (Unified Nlp) : Wi-Fi and cell tower connections using geolocation, Maps API (maps v1) – replacement of Google map, Store (Phonsky) which gives access to store to download apps, K-9 mail, ProtonMail and DuckDuckGo search engine Open Street Mapping creates free editable map of the world but the drawback is Lineage OS still allows the installation of Google Apps. Maksim Zavgorondii, Nikita S. Ivanov, Igor V. Latypov, Aleksey Zhavoronkov In [5], have discussed through the flowchart of boot sequence of android as given below:

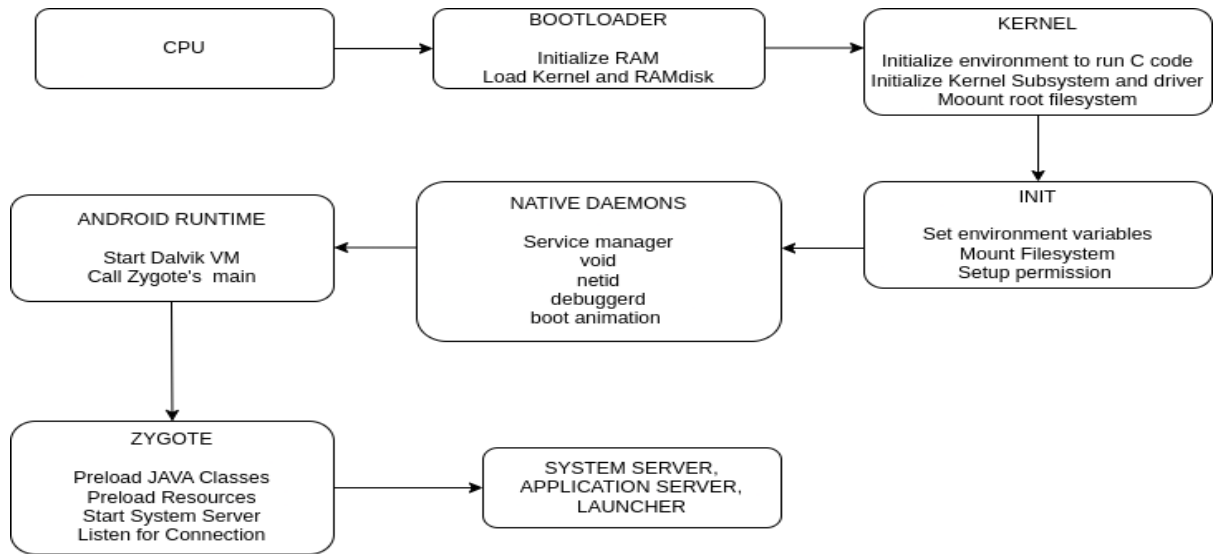


Fig. 3: Bootloader

The first step of boot sequence is CPU, then in to the bootloader where RAM is initialized. Then the sequence moves to kernel where file systems are mounter, and the environment variables are initialized. Then Zygote is called upon in the Android Runtime and the system boots.

However the system partition of corporate ROM is kept unencrypted because it doesn't include important corporate files. However, user can insert in system folder third party scripts or delete scripts which are used to provide protection of corporate ROM. Therefore, it is necessary to provide an integrity check of the system partition which will check if partition was changed.

V. METHODOLOGY

A. DEVELOPMENT PHASE

1. Setting Up Build Environment

- Setup Linux to build Android
- Setup repo

2. Downloading The AOSP Source Code

- `mkdir foldername && cd folder name`
- Recommended: adding `---depth=1` between `repo init` and `-u` in order to make a shadow clone of the source (will reduce drastically the space used).
- Paste it into a terminal under the folder you've just created and hit enter.
- `repo sync --current-branch --no-clone-bundle --no-tags --optimized-fetch --prune --force-sync -j$(nproc --all)`

3. Download The Device Trees

In the ROM folder, there is a hidden folder called `.repo`. So, to be able to download the device trees:

```

cd .repo
mkdir local_manifests && cd local_manifests
nano zbuild.xml
    
```

4. Build the ROM

B. DEPLOYMENT

1. Unlocking the BootLoader

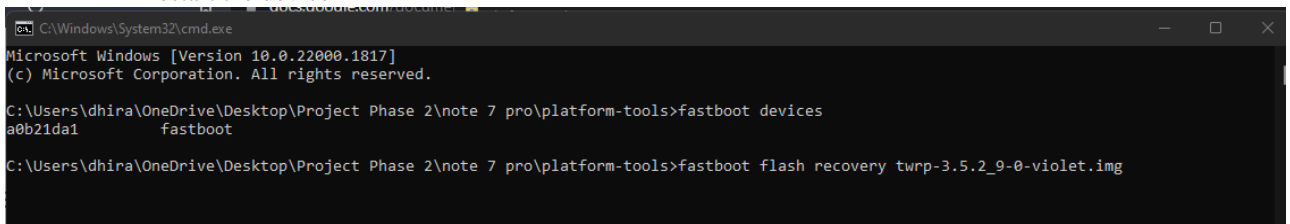
- a. Enable the Developer Options by tapping the Build Number of the Phone more than 5 times in Settings>About Phone> Build Number.
- b. Enable the USB Debugging
- c. Toggle the OEM unlock Button
- d. Unlock the bootloader using the unlock tool provided by the respective phone manufacturer.

2. Setting up the adbflashtool

- Install the adbfastboot drivers.
- Download the adb flash tool zip folder.

3. Flash the TWRP or OrangeFox recovery tool

- Open cmd inside the adbflashtool folder
- Connect the phone in fastboot mode by pressing the power button and volume down key for 5 seconds or more and using a fast USB cable.
- type the command “fastboot flash recovery twrp.img”
- restart the device



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.1817]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dhira\OneDrive\Desktop\Project Phase 2\note 7 pro\platform-tools>fastboot devices
a0b21da1          fastboot

C:\Users\dhira\OneDrive\Desktop\Project Phase 2\note 7 pro\platform-tools>fastboot flash recovery twrp-3.5.2_9-0-violet.img
```

Fig. 4: adbflashtool

4. Boot into the recovery mode by pressing the volume up and power button for 5 seconds or more.
5. Copy the Custom OS in the phone by using the command “adb push projectdeGoogled.zip /sdcard”
6. Go to wipe > advanced wipe and select Dalvik cache, cache, system, vendor and data and swipe to wipe.
7. Go to install and select the OS zip file (project deGoogled OS) and sipe to install the OS.

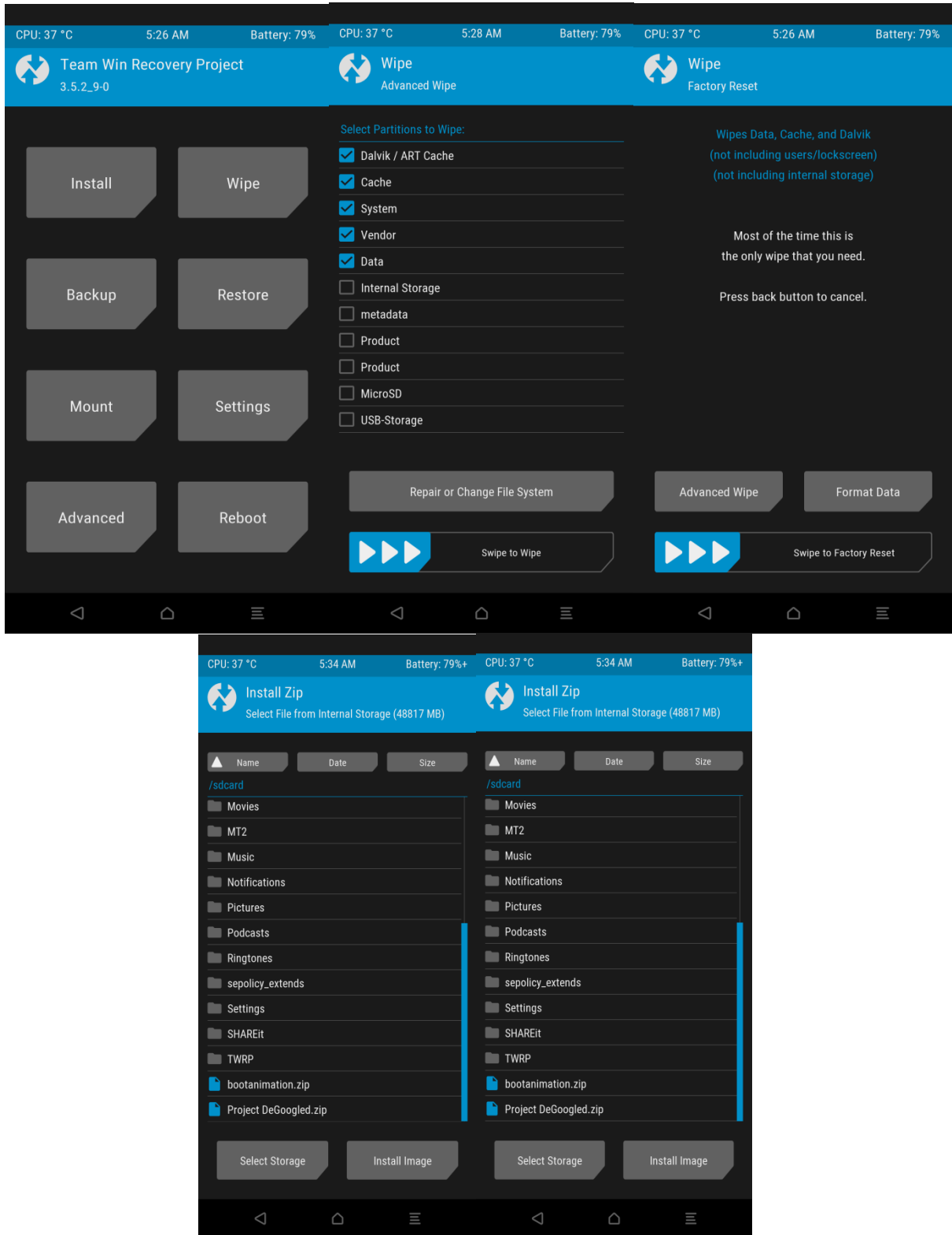


Fig. 5: TWRP Recovery for installation of OS



VI. CONCLUSION AND FUTURE WORK

Since in this age of "PRIVACY IS A MYTH", its is very important to secure the personal data, but even without our consent and knowledge, Companies like alphabet (Google) and Meta (Facebook) access our data and details like Biometrics, passwords, location, websites we access and our entire activity on the web and online and sell the data to advertising companies for advertisement purposes. In such case, a de google android OS is the best possible Solution. Since a de-googled phone does not include any of the services provided by the google and instead of Google Mobile Services, use third party open source software services and search engine, and also users can select and install applications that they think are safe for them, without google having any control or access to any hardware, software or data control. It provides users more freedom to choose and use the apps that are safe for them.

REFERENCES

1. Developing Custom ROM based on Android using AOSP ,NMAM Institute of Technology ,Shreyas S. August 2020
2. Empirical Research And Auxiliary Tool For Custom Android ROMs, Jinan University, Muhammad Suleman, Xiaojian Zhong, Yuxia Sun ,2020
3. Custom Android ROM's ,ShriS'ad Vidya Mandal Institute of Technology, Gujarat Meet Kumar Rajendra Kumar Parekh ,March 2022
4. Lineage OS Open Source Mobile OS, Challenges and Strengths ,Asian Institute of Technology, School of Engineering and Technology, Thailand ,Rajashekhara Ponakala, December 2017
5. Creating the Corporate Android Firmware Using Dual boot Mechanism, California State University Maksim Zavgoronddii, Nikita S. Ivanov, Igor V. Latypov, Aleksey Zhavoronkov July, 2021



Impact Factor: 8.379



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details