Android Operating System and its Security Issues

***Piyushi Gulati*[1]*, Kamini Kumari Rana*[1]*, Surabhi Raghuvanshi*[1]*, Dr Anupama Pankaj*[2]**
[1]*PG Students, Department of Computer Science and Technology, MRIIRS, Faridabad, Haryana, India*
[2]*Associate Professor, Department of Computer Science and Technology, MRIIRS, Faridabad, Haryana, India*
***Email**: piyushi.gulati@gmail.com*

***DOI:** http://doi.org/10.5281/zenodo.2605874*

Abstract

Android is a Mobile and Tablet Operating System premised on the Linux kernel owned by Google. The ultimate innovative feature of Android Operating System is open source due to this anyone can publish their applications freely on the Android market. This openness introduces the broad number of developers which utilize this platform, but it comes with the hazard that user may download malicious software which is written by network hackers and harm to its privacy. This requires the study of the Security Mechanisms for Android and to make it easy and user-friendly to make the user aware of areas where he has to be cautious. This paper gives an idea about the architecture of the Android operating system, security features of an android, security issues faced by the Android and solutions for security issues of the Android operating system.

***Keywords:** Android, architecture, security, security solutions*

INTRODUCTION TO THE ANDROID OPERATING SYSTEM

The Android platform works on Linux kernel. The Linux kernel has gained popularity for years because of the security features. Also, the Linux kernel provides a level of abstraction between the device and hardware [4]. This level of abstraction provides all the necessary hardware drivers like display camera, keypad etc. Figure 1 shows the Android operating system architecture.

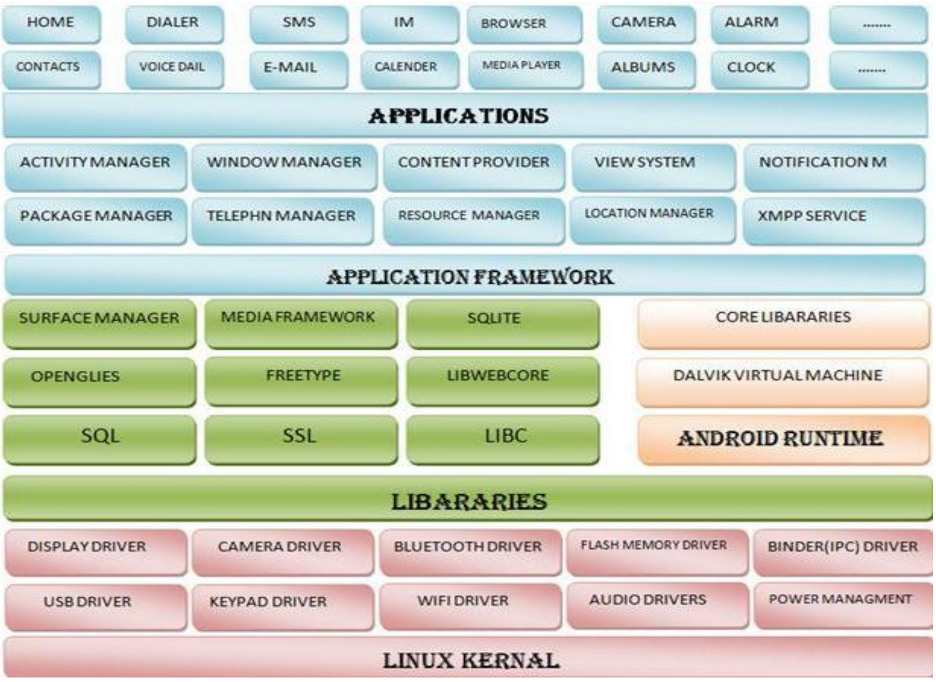


***Figure 1:** Architecture of the Android Operating System.*

The subsections below discuss the various components of the Android operating system

Linux Kernel

At the bottom of the android architecture is the Linux kernel. This layer acts as an interface between hardware and the user. It manages all the activities, memory and sharing of resources .this layer is mostly used by hardware manufacturers as it provides a hardware abstraction layers remain unchanged despite changes in the underlying hardware.

Mobile devices have limited memory space. Therefore it is very important to have a Linux kernel service for memory management.

Libraries

A set of libraries sit on top of Linux kernel. These libraries contain Surface Manager, SQLite, WebKit, well-known library libc, Media framework, Free Type, SSL etc. These libraries are written in c or c++ and called by java interface [1].

These libraries provide the following functionalities:-

- The Surface manager to manage the display of devices.
- SQLite database act as storage for Android for repository.
- WebKit provides an open source web browser engine.
- Libc contains C libraries.
- Media framework enables playback and recording of popular audio /video formats. It also provides support for static image files [1].
- SSL libraries to provide Internet security.

Android Runtime

Android runtime is the second layer from the bottom. Android runtime includes a set of core libraries and DVM that is Dalvik Virtual Machine [4]. Dalvik Virtual Machine is a kind of Java Virtual Machine which is created especially for the Android [4].

Dalvik Virtual Machine is developed especially for mobile phones [1]. Dalvik Virtual Machine like Java Virtual Machine. Java virtual machine allows the computer to execute java codes as well as other programs written in different languages and compiled to java byte code but for mobile phones [13]. The other difference between the two is Dalvik virtual machine is register-based whereas Java virtual machine is process based.

The Dalvik Virtual Machine uses the of Linux core characteristics such as memory management, Portability and Multi Threading, which is a prominent feature of Java language. Dalvik virtual machine works on low memory and low processing power environments.

The Android runtime also permits Android developers to write applications on Android by providing a set of core libraries using Java programming language.

Application Framework

The Application Framework allows many higher-level services and the systems which can be used by android developers to build innovative applications.

The Application Framework is a set of basic tools with which a developer can build more complex tools.
The Android framework includes the following key services −

- **Activity Manager** −Itmanages the lifecycle of activity. It provides the user an interface to interact with the application.
- **Content Providers** −Content Provider is your Android system’s middleman and [18].
- Permits apps to communicate and share data with various apps.

- **Resource Manager** –It manages the varioustypes of resources such as layout files, strings and graphics which can be used in developing new applications.
- **Notifications Manager** –It enablesapplications to show alerts and notifications to the user which appears on the screen.
- **View System** −it provides rich and extensible views such as button, grids, textboxes etc. used to design user interfaces for an applications.

Applications

The user can code the applications and can install in this layer. Some of such applications are contacts, camera, calendar, media player, Web Browser, and Alarms etc.

DIFFERENT SECURITY FEATURES OF ANDROIDOS

The Android operating system is popular because of the security features. The following are the security features
provided by the Android to its users:

1. Security at operating system level
2. Application sandbox for all applications
3. Security in interprocess communication
4. Application signing
5. Application defined and user-granted permissions

Linux Kernel

As the Linux is open source software it was constantly researched, attacked and modified by many research developers. After a lot of modifications Linux has become secure and stable kernel. Linux kernel imparts Android with various key security features including:

A user-based permissions model for each file and directory. In Linux there are 3 user-based permissions: Owner, Group, Other users.

1. *Owner* - The Owner permissions for theowner of the files or directories.
2. *Group* –The group permissions for the groupthat has been given the files or directories.
3. *Other users* - The other Users permissionsapply to all other users on the system.
   Every file or directory has three basic permission types:
4. Read- The read permission refers as the usercan read the contents of the file
5. Write - write permissions refer as the user canto write or edit the files or directories.
6. Execute - The execute permission refers as theuser is allowed to execute the files or view the contents of directories.

This permission model makes sure that these security features are maintained while accessing Android files.

a) Process isolation: It as a separate process which executes the applications by assigning a special user Id (UID) to each android application.
b) A secured mechanism for secure Inter Process Communication.
c) A unique feature to eliminate non-essential and vulnerable parts of the kernel.

The Application Sandbox

An application sandbox is a security mechanism executing the untested codes or programs from un-trusted users and un-trusted websites. The sandboxing technique permits limited access to device’s resources [1]. This way security of the system is improved [1]. This technique provides platform to execute malware code also it doesn't allow the software to harm the host device [1]. This is done by providing access to only those resources for which permission is granted [1].

Secure Inter-process Communication

Inter-process communication is the mechanism which allows Android components to communicate with each other.

Instead of using the old Linux techniques such as file system, network sockets and shared files forinter-process communication, the Android operating system provides the latest techniques for IPC such as Services, Intents, Content Providers and Binder [3].

Application signing

The applications to be run on the Android operating system must be digitally signed so that the developer of the application can be identified. Application signing feature also builds a trust relationship between applications.

Application-defined and User-granted Permissions

Permissions is one way of providing security to Android based applications. By default, No permissions are granted to the android applications, and this makes them secure. The Protected APIs include Location data (GPS), SMS/MMS Functions, Bluetooth Functions, Camera Functions, Telephony Functions, and Network or data connections [1].

SECURITY ISSUES FACED BY ANDROID

1) **Malicious Applications:** The Malicious Applications are causing serious problems. Some of these Applications can reveal the Smart phone user's location, contacts, confidential information and other personal information. These Malicious Applications will download other Malicious Applications from the Internet. This exposure of private information can breach the individual security.

2) **Unsafe websites**: Some websites may contain anumber of Malicious Applications. Any user of an Android smart phone who uses the browser to surf the Internet may be exploited if he/she visits a malicious webpage and the attacker can run any code with the help of any browser.

3**) Data security of mobile devices**: smart phones are different from desktop computers because of their portability and therefore they are at a higher risk of loss. When any user lost his device, the data on the devices is not easy to recover.

4) External storage: The major security issue of themobile phones is the protection of the files created on the External Storage, such as Secure Digital Cards (SD cards). The files on SD cards are globally readable and writeable and it can be removed and modified by any user.

Network data security for mobile devices

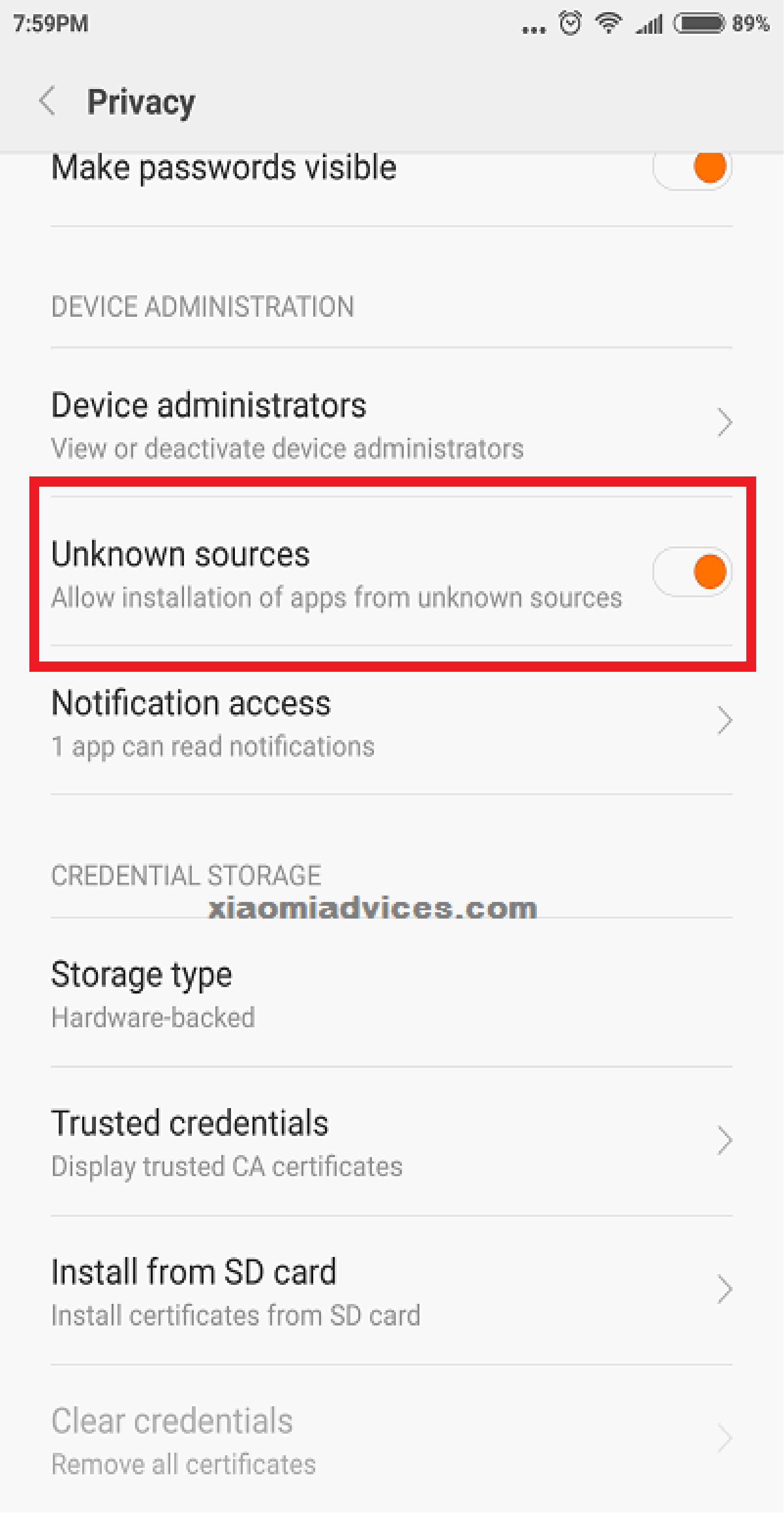
The use of open wireless connections can make the attackers or hackers extract the user’s personal information that can be used to access their bank account details and other secure information.

SOLUTIONS FOR SECURITY ISSUES OF ANDROID OS

Not Using External Storage

Files created on removable storage, such as SecureDigital cards (SD Cards), are globally readable andwritable. Because removable storage can be removed by the user or others and also modified by any other application, the user should not store sensitive information using removable storage.

Disable Unknown Sources Option in Android



7:59PM ... 89%

Privacy

Make passwords visible

DEVICE ADMINISTRATION

Device administrators
View or deactivate device administrators

Unknown sources
Allow installation of apps from unknown sources

Notification access
1 app can read notifications

CREDENTIAL STORAGE

xiaomiadvices.com

Storage type
Hardware-backed

Trusted credentials
Display trusted CA certificates

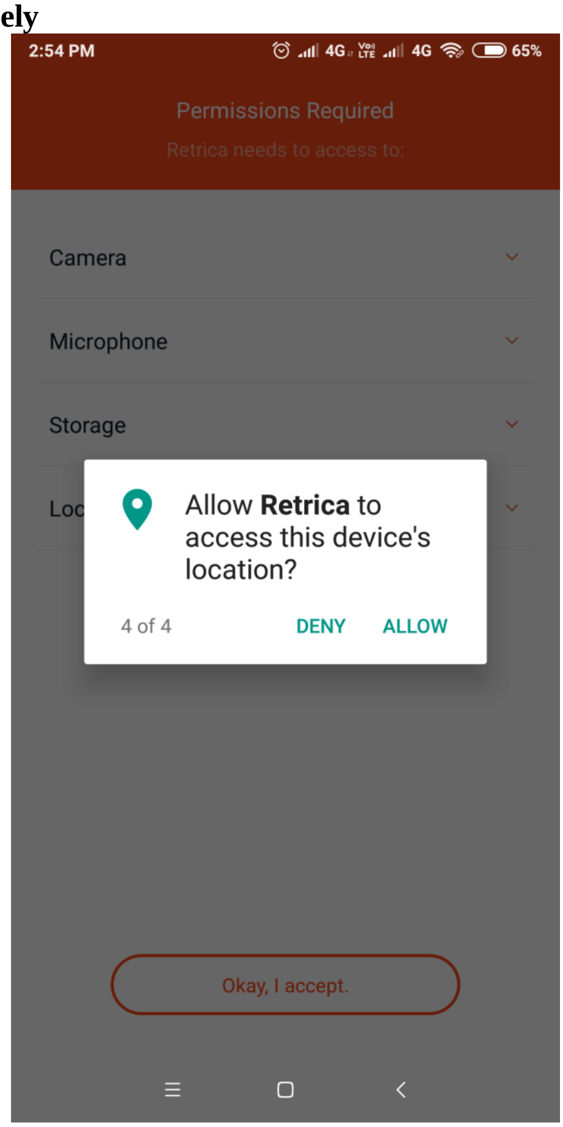
Install from SD card
Install certificates from SD card

Clear credentials
Remove all certificates

Figure 2: *Disable Unknown Sources Option in Android.*

When user is trying to install an app on any other websites rather than Google play store, the message "UNKNOWN SOURCES" should pop up and it should have option for enabling or disabling the installation. For maintaining the security try to download applications from certified sources only like Google play store in Android platform. For the security reasons, it is already been disabled by default.

Grant Permissions Wisely



Allow **Retrica** to access this device's location?

Figure 3: *Grant Permissions.*

When the user install an app from Google’s Play Store, a pop-up listing all the permissions the user requires pop up. This could include permissions like access to the user text messages, phone call details, media files, etc. Sometimes applications require permissions that are not acceptable, for example, some camera application requires the user’s phone contacts. By giving these permissions it can lead to information leak. So read carefully all the permissions before the installation an application.

Data Encryption

For maintaining security, encrypt or password protects your confidential data so that it cannot be accessed by some other user.

Keep your apps up-to-date

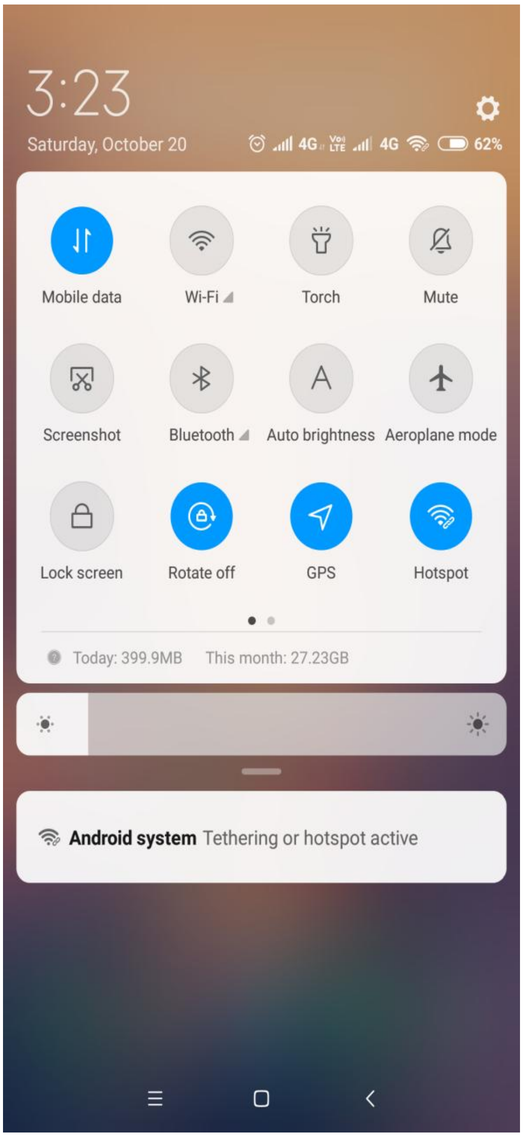
Users should update their applications as soon as the newer version of an application is available. The newer version applications have several bugs fixed. A newer version is released after any vulnerability in an application is detected and rectified by the developers. This also improves the efficiency of the device.

Use an Antivirus App

A user should install an antivirus application so that the malicious files can be detected and destroyed. Several antivirus apps for Android are avast, Norton, quick heal etc.

Disable GPS Option in Android

User should disable the GPS option in android when it is not necessary because sometimes other applications access the smart phone's location unnecessarily and uses more battery power and mobile data due to this cybercriminals can track the user's location and use the location information for their criminal purpose. Therefore, users turn on the GPS only when it is necessary.



Today: 399.9MB This month: 27.23GB

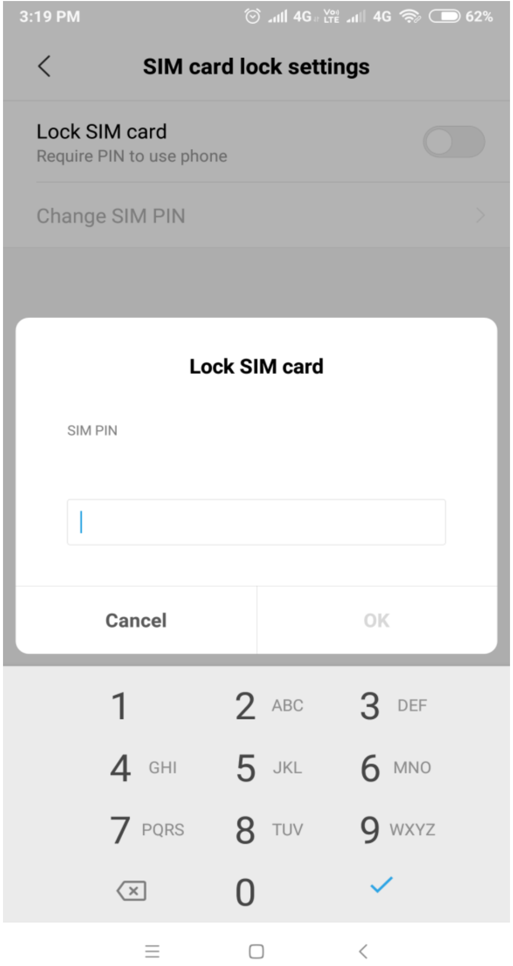
Android system Tethering or hotspot active

Figure 4: *Disable GPS Option in Android.*

Enable SIM Card Lock

Disable the SIM card lock option in android allows the thief to gather information about user's identity because phone numbers are used as an identifier to create social media accounts, sites and apps etc. Cybercriminals can change the password and get access to the accounts and also bank accounts by using text message based authentication and OTP (one time password).

For example:-Facebookaccount can be accessed by using the “forgot password” option at login page which sends the security code to the phone number. Therefore, users should enable the SIM card lock to protect the accounts and identity.



3:19 PM

SIM card lock settings

Lock SIM card
Require PIN to use phone

Change SIM PIN

Lock SIM card

SIM PIN

Figure 5: *Enable SIM Card Lock.*

CONCLUSION

The Android operating system is one of the most popularly used operating system and will probably be around for many years to come. As Android-based Mobile Devices become more advanced, they continue to have more uses and that’s why more information stored on them. So, it is important for users and developers to understand the security risks and what they can do to protect their personal information. Users need to aware about of all the application what they are installing on their device and think wisely before giving permission to applications. Developers need to take the proper improvements to prevent any security breaches or issues. Currently Developers are working to enhance the Android security in the new version of Android “P”. Google wants to add a little more "privacy and security" to Android P.

REFERENCES

1. https://pdfs.semanticscholar.org/11f4/b8efd1a9af746 f17ac5e8d6a789bd3c3a9b7.pdf
2. https://www.scribd.com/document/208852386/Cc-4201519521
3. https://vdocuments.mx/documents/android-vulnerability-to-impersonate-trusted-applications.html
4. https://www.quora.com/What-is-the-Android-application-Architecture

5. https://stackoverflow.com/questions/10283725/what-is-difference-between-software-stack-and-os-why-android-is-not-an-os-but
6. https://www.researchgate.net/profile/Carlos_Carrascosa/publication/221611128_Does_Android_Dream_with_Intelligent_Agents/links/00b495176646066162000000.pdf?disableCoverPage=true
7. https://www.scribd.com/document/262130241/Android-vulnerability-to-impersonate-trusted-applications
8. http://www.academia.edu/6499341/CC4201519521
9. https://www.safaribooksonline.com/library/view/android-malware-and/9781482252200/chapter-09.html
10. https://www.reddit.com/r/MotoG/comments/7twx9 9/any_news_of_the_oreo_update_on_moto_g5_plus/
11. https://www.researchgate.net/profile/Ben_Benjamin/publication/264751361_Penetration_Testing_for_Android_Smartphones/links/53edf0260cf26b9b7dc63766/Pe netration-Testing-for-Android-Smartphones.pdf
12. https://en.wikipedia.org/wiki/Java_virtual_machine#C_to_bytecode compilers
13. https://tailforwindows.org/download-file/java-programming-with-oracle-sqlj
14. https://www.studypool.com/discuss/6251152/os-mechanisms-that-handle-deadlocks-etc
15. http://www.ijfeat.org/papers/march20162.pdf?i=1
16. https://quizlet.com/215337386/bcis-chapter-7-review-questions-flash-cards/

Cite this article as: *Piyushi Gulati, Kamini Kumari Rana, Surabhi Raghuvanshi, & Dr Anupama Pankaj. (2019). Android Operating System and its Security Issues. Journal of Android and IOS Applications and Testing, 4(1), 1–9. http://doi.org/10.5281/zenodo.2605874*