THE ANALYSIS OF IMPLEMENTATION OF CUSTOM FIRMWARE, MICROG, AND HOST ADBLOCKER ON PRIVACY LEAKING ON ANDROID OPERATION SYSTEM

Rizki Perdana Bowo Laksono
Accounting Department, Yogyakarta State University
rizki.perdana2016@student.uny.ac.id

Abstrak: Penelitian ini bertujuan untuk: (1) memahami bagaimana kebocoran privasi terjadi pada perangkat android, (2) mengetahui cara melakukan perlindungan privasi pada perangkat android dengan menggunakan komponen library custom firmware, microG, dan host Adblocker. Penelitian ini merupakan uji coba penerapan teknologi di bidang Android menggunakan pendekatan deskriptif kualitatif. Tahap dari penelitian ini antara lain: 1) perencanaan, 2) implementasi, dan 3) analisis. Pada tahap pengembangan perlindungan privasi pengguna Android, penelitian ini menguji pada dua set perangkat Android untuk membandingkan perbedaan dampak kebocoran privasi. Masing-masing perangkat dipasang aplikasi keuangan digital yang sama. Dari hasil penelitian menunjukan bahwa perlindungan privacy menggunakan custom firmware, microG, dan host adblocker dapat menurunkan aktivitas kebocoran privasi yang dilakukan oleh perangkat Android. Dilihat dari hasil analisis menunjukan adanya penurunan jumlah privacy tracker dimana pada perangkat tidak dilindungi memiliki privacy tracker sebanyak 20 tersebar pada 15 aplikasi dan pada perangkat yang dilindungi hanya ada enam privacy tracker yang tersebar pada lima aplikasi.

Kata kunci: Privacy Leaking, Android, Custom Firmware

Abstract: *This research aims to: (1) Understand how privacy leaks occur on Android devices, (2) know how to do privacy protection on Android devices by using custom firmware library components, microG, and host Adblocker. This research is a trial experiment of the implementation of technology in the field of Android using a qualitative descriptive approach. The phases of the study include 1) planning, 2) implementation, and 3) analysis. In the development phase of Android User Privacy protection, this study tested two sets of Android devices to compare the difference in privacy leak impact. Each device is installed in the same digital financial application. The research shows that privacy protection using Custom Firmware, MicroG, and host adblocker can decrease the privacy leak activity performed by the Android device. Judging from the results of the analysis showed a decrease in the number of privacy trackers in which the device is not protected have a privacy tracker as much as 20 scattered on 15 applications and protected devices there are only six privacy trackers scattered on five apps.*

Keywords*: Privacy Leaking, Android, Custom Firmware*

INTRODUCTION

Android helps the advancement of communication technology by creating a smartphone. The existence of Android has succeeded in creating a digital ecosystem for software developers to take advantage of opportunities to create applications for smartphone technology. This progress is made possible because Google opening it's Android source, software developers no longer need to pay for expensive software certifications or share the profits of selling applications on a market platform. The rapid development of the Android smartphone market share shows evidence that high consumer demand for smartphone technology. This is not surprising, considering the development of the Android

mobile market share accompanied by the rapid growth of application and game development on smartphones [1].

Distributing smartphone applications through digital application market platforms can benefit end-users because users can choose from the wide variety of applications available on the application platform market [2]. Popular application market platforms include the Play Store as an official distributor of applications for Android-based smartphones and the App Store as an official distributor of applications for the iPhone. Although most of the applications distributed do not violate user privacy, a study conducted by Arp et al [3] found that there are hundreds of android apps that have been detected that violate the user's privacy. Furthermore, Android is indeed an open and most popular platform from other mobile platforms. According to Rusello, Android is the most perfect environment to exploit and spread attacks on system security [4].

Android's popularity is not only in its security flaw but is entering the realm of human life where most of the activities of communication, financial transactions, banking, and all kinds of business activities are carried out through Android phones. Based on data from OJK, katadata.co.id, OVO, GOJEK, and LinkAja (Pusparisa, 2019) shows the development of financial technology (fintech) very fast in Indonesia. Observations made on the Google Playstore platform noted that the number of downloads for the Go-Pay application by GoJek had already reached 50 million downloads, followed by OVO and LinkAja as many as 10 million downloads. The high interest of Android users in Fintech applications forces application developers to increase application security [5].

Because the Google Android operating system provides a permission-based security model that limits application access to users' data. Every application that is newly installed or already installed will request access to sensitive and functional system data to execute commands such as asking permission to access telephone data, access files, access GPS locations and part of it. If access permission is not granted then the application cannot be used, then the user is forced to grant access permission to the application so that he can still enjoy the service even though the user's data is at stake. In addition to enforcing access permissions, Android users who carelessly give access permissions to applications clearly do not understand the sensitive data used by installed applications. Things like leakage of personal and sensitive data on Android users is one of the consequences of arbitrary permissions by users.

To protect the privacy of user data, Android combines various security mechanisms and features that allow the protection of some users' privacy from applications that run privacy data theft mechanisms. However, developing a security system model for battery-powered electronic devices that is suitable for all devices is not an easy matter. The Android operating system itself still has various security problems, even the Android security system model still has a variety of shortcomings [6].

Problems with the Android security system have been covered several times with several additional security modules such as User Permission [7], AppFence [8], and FlaskDroid [9]. However, research conducted by Enck, et al [10] still found a leak of important information from Android users from using the security extension.

Thus to enhance privacy protection, researchers propose the implementation of Custom Firmware, MicroG, and Host Adblocker to overcome the problem of leakage of data privacy of Android users. Firmware is a software contained in a computing system that functions to provide the lowest level of control for certain hardware, on the Android operating system firmware is defined as a set of binary systems written on a fixed storage device, usually, the Android firmware is installed in the eMMC (embedded MMC) storage inside the Smartphone [11].

Firmware is also referred to as Read-Only Memory (ROM), as the name implies ROM means software that can only be read without being modified again by the user of the device, ROM is very rarely replaced during the life of the system except in the process of upgrading the ROM [12]. Based on the manufacturing, ROM is divided into two namely Stock ROM and Custom ROM, stock ROM is the original firmware of the device that is usually already pinned by a vendor or manufacturer on a Smartphone device [13].

Stock ROM offers better system stability than Custom ROM because before being released to the market, functional software inside the Smartphone will be tested many times to ensure there are no bugs and errors on the entire smartphone device [12].

On the other hand, Android with Custom ROM is no more stable than Stock ROM because most of Custom ROM is developed by the Android activist community which consists of only a few people, especially the Custom ROM developer community has no commercial purpose in making ROMs so that each ROM version released free to end-users [14]. According to Sun, Cuadros, and Beznosov [15], some Custom ROM giving an access to root directory, rooting is a process that allows

Android device users to obtain special, ongoing control over the device, if the device has been rooted, the user of the device has access to remove system restrictions that are implanted by the Android Smartphone vendor, change or delete vendor default system applications, run paid applications for free, and get functional Root access that is not owned by Smartphone Android without Root such as the data backup feature. and periodic applications, firewalls, anti-malware, queuing privacy tracking, overall smartphone performance improvements and regular update [16].

Custom ROM has several types some of the most widely used are LineageOS, OmniROM, Paranoid Android, Resurrection Remix OS, Pixel Experience, and AOSP Extended. From that list, researchers chose LineageOS as the base of Custom ROM to be used in this study because LineageOS supports 255 Android devices from various brands and types, has a user privacy protection feature known as Trust, is more stable than other Custom ROMs due to the community a large developer, and LineageOS is frequently updated regularly to maintain system security and feature enhancements, and finally, LineageOS was developed without the default Google application along with Bloatware that was never actually needed by the user [17].

LineageOS was developed from Google's AOSP (Android Open Source Project) source code, LineageOS can operate without using Google's proprietary software such as Google Chrome, for example, LineageOS replaces all Google default software with open source applications ranging from file explorer to internet browser. However, one obstacle for all android ROMs that do not use Google's proprietary software known as GApps (Google Apps) makes Android devices unable to run certain applications that require GApps such as banking applications, e-money (Funds, OVO, LinkAja), Pokémon GO, Mario Run, map applications, and several other applications. For this reason, the software is needed that can replace the GApps function, namely MicroG. Google does make AOSP an open-source project whose source can be developed by anyone, but the main core of AOSP is locked by Google so that the GApps application in AOSP is not deleted or replaced by other applications. For this reason, LineageOS which does not have GApps requires MicroG software to replace the GApps function.

If LineageOS can be paired with MicroG, why can't LineageOS be paired with GApps? According to Conway [18], the underlying reason for the development of MicroG is the distrust of Android users on Google's GApps. Google's regulations

explain that Google provides all its services free of charge to users and that instead all user data will be used for commercial purposes Google and Third-Parties services or third parties that users use. Considering that each user data is very sensitive, many Android users choose to use Custom ROM with the addition of MicroG to maintain functional Android devices without the need to depend on GApps that jeopardizes personal data.

From the above explanation, LineageOS briefly functions to replace the Stock ROM installed on Android devices and MicroG is used to replace the GApps function. Functionally LineageOS and MicroG already function like Android with Stock ROM without any leakage of user's data, but there is still a threat of privacy leaks that can be done by third-party applications, such as social media applications, video games, and other additional applications. For this reason, additional mechanisms are needed to ensure that there are no privacy leaks by third parties. According to Kim [19], There are two ways to block private data access by third parties, namely using the Non-Root method and the Rooting method. Non-Root method is more appropriate to use for smartphones that have not done the Rooting process, this is because the Non-Root method process does not require superuser access to block the privacy tracker of third parties, the way the Non-Root method works is to modify the Android Smartphone network connection to connected to the Virtual Private Network (VPN) of the Non-Root application so that the data sent and received by the Smartphone is filtered first, leaving only the data needed without tracking data. Examples of applications that use the Non-Root method include Blokada, AdBlock Plus Browser, Brave, DNS66, and others. But the drawback of this method is that it can interfere with network stability and the performance of other applications and this method consumes more battery power.

While the Rooting method can work more effectively without disturbing application performance and Smartphone network stability, the best-known Rooting method is to reverse engineer the "/ system / etc / hosts" file on the localhost system to block each data tracking domain and advertiser. Although effective, one disadvantage of Rooting is that this method can only be applied to Androids that already have Rooting access. The most popular application for blocking user data tracking access by the Rooting method is AdAway. AdAway is an Android software that has an open-source and free that can be used by anyone, the way these software works is by adding the domain you want to block access through the host file that is modified using

AdAway, thus this method is better known as Host Adblocker [20].

The testing method is appropriate for Xiaomi-based Android smartphones because most Xiaomi products, especially the Redmi variant, carry the MIUI operating system which has bloatware and privacy tracker embedded in the system [21]. Based on reports from various international media sites India Today Tech [22], Gadgets Now [23], and Decca Chronicle [24] reveals how Xiaomi collects personal data of Xiaomi Smartphone users secretly without the user's knowledge, after the news was revealed in public Xiaomi revealed an apology to all Xiaomi users around the world [25]. Nevertheless, Xiaomi still collects user personal information for Xiaomi's business needs, this is written in the company's privacy policy which states that every user's data stored in the Smartphone will be collected and used for the benefit of the company [26].

The effects arising from the theft of important data Smartphone users are not limited to the behavior of hacking attacks, acts of flooding unimportant information or spamming, so that the most severe is the act of scamming online fraud behavior that is possible because user data is misused by certain parties. For this reason, this study aims to analyze the overall application of reverse engineering on Xiaomi smartphones, starting from the application of Custom ROM, MicroG, and the application of Host Adblocker to prevent privacy leaks on Android Smartphones.

LITERATURE REVIEW

Privacy Leaks

Fundamentally, the rules of Article 28 l Paragraph (1) of the 1945 Constitution and the international constitution Right to Privacy agree that privacy is the right of all humans, every individual has the right to save their data for their own needs and not give it to anyone. The written rules of the Right to Privacy Constitution that are internationally agreed on the state that anyone who takes or uses a person's data without the permission of the owner of the personal data is included in human rights violations and should have consequences for those human rights violations.

Moore [27] explains that privacy is the right to control access to places, locations, and personal information by using controls for an item. This opinion is supported by Spiekermann [28] which explains that privacy is the ability of individuals to control information about themselves.

According to Gibler [29] defines that privacy leaks are conditions where personal information or a unique identifier about the device sent out leaves the device without the

user's permission. Furthermore, Li [30] defined the privacy leak as a path to sensitive data called source, which causes something to send data out of an application or device. Kim [31] also define that privacy leaks are a flow of personal information that is sent out without permission from the device through the network, file, or short message service (SMS).

Based on the explanation above, it can be concluded that Privacy Leaks is a condition where personal information or information about the device sent out leaves the device without the user's permission. Android-based smartphones are the most vulnerable to privacy leaks because of the huge number of users compared to other smartphone users and many third-party developers infiltrate specific scripts to send user data without permission [32], therefore researchers are interested in analyzing privacy leaks on Android smartphone.

CUSTOM FIRMWARE

To trace the privacy leaks on an Android device it needs to be traced from the root first, in this case, the operating system of the Smartphone device namely Android. Operating system or known as firmware is a software contained in the computing system that functions to provide the lowest level of control for certain hardware, the Android operating system firmware is defined as a set of binary systems written on a fixed storage device, usually, the Android firmware is installed in storage eMMC (embedded MMC) in a Smartphone [11].

The term firmware for Android is better known as Read-only memory (ROM), which is a memory that can only be read by the system and cannot be modified from within and without superuser permission. Android firmware was developed from Google's open-source code, the Android Open Source Project (AOSP). Every vendor, community, and individual has the freedom to use the AOSP source code to develop a ROM.

MicroG

The tagline of MicroG is "A free-as-in-freedom re-implementation of Google's proprietary Android user space apps and libraries" which means the user's freedom to use applications and libraries from Google's proprietary. Sourced from the official website microg.org that Google Apps is proprietary software that locks the Android ecosystem so that every third-party app must use GApps so that applications can function within the Android ecosystem. Due to the imposition of Google's ecosystem, various open-source applications also use GApps so that the application can run on the Android operating system.

The worst scenario that can happen if an Android Smartphone does not use GApps then third party applications will not be able to work in it, thus forcing every company, manufacturer, vendor, community, and end-user to embed GApps in Android.

To overcome Google's monopolistic behavior in the Android operating system, the MicroG development team created a set of systems to replace GApps performance. So that Android without GApps can still function normally.

Host AdBlocker

even though the Android operating system is free from internal bloatware, there is still a privacy tracker that poses a threat to user privacy by third parties app, so additional protection is needed to block privacy tracker access in the Android operating system. Based on research conducted by Merzdovnik [20] There are three methods to block access by privacy tracker: Network-Based Blocking, Browser Extension, and Different Types of Rulesets. Because this research ecosystem uses an Android device for that the proper method to use is Different Types of Rulesets namely by implementing centralized ruleset which is proven superior in blocking privacy tracker in the Android operating system. To implement centralized ruleset in the Android operating system, root access is needed in the domain transfer system in android, namely in the "system / etc / host" file.

RESEARCH METHODS

This research uses the approach of trial methods and qualitative descriptive analysis. Descriptive research is a method of study that is used to find a broad-scale knowledge of research objects at a particular time [33]. The description of qualitatively descriptive analysis is used to describe the entire network implementation process of the libraries until the impact on Privacy Leaking protection of third-party applications

To ensure the results of these experiments can be proven accountable, then the research should use methods or tools that support the readability of the research results. Therefore, researchers use a tool developed by Razaghpanah et al [34], the Lumen Privacy Monitor, to record each transmission of data inside the smartphone and bring out the results in the form of analysis reports in real-time.

RESULT AND DISCUSSION

The purpose of this study is to analyze the results of the implementation of Custom Firmware, MicroG, and Host Adblocker on privacy leaks on Android smartphones. The research tests several popular financial applications where the digital wallet applications mentioned in the previous

chapters have virtual money balance and payment features. Thus, the privacy protection of this application needs to be kept tighter so as not to harm the user due to a phishing attack.

This research uses the approach of trial methods and qualitative descriptive analysis. Descriptive research is a method of study that is used to find a broad-scale knowledge of research objects at a particular time (Shah, 2010). The description of qualitatively descriptive analysis is used to describe the entire network implementation process of the libraries until the impact on Privacy Leaking protection of third-party applications

This chapter will explain how the custom firmware, MicroG, and Host Adblocker implementation processes are implemented on Android smartphone devices, the explanation covers how to find out and analyze leaks privacy data using the Lumen Privacy monitor. Next, the experimental results will be explained in the discussion.

Before conducting research, several things need to be prepared by researchers. Some of these include:

1. Research Device

Following the explanation of the research method, this research uses two Android Smartphone devices, for android smartphones used for the experiment is Xiaomi Redmi 4X.

2. Necessary application and files

a. Custom firmware file, MicroG file, and Custom Host Adblocker

When this research was conducted, researchers used LineageOS custom firmware Version 16.0, MicroG Service Core Ver. 0.2.10.19420, and the host file from https://energized.pro/. The three components of the file are implemented on smartphones Xiaomi Redmi 4X.

b. Measuring and analyzing application

The application used to measure and analyze the research data this time is Lumen Privacy Monitor version 2.2.2 with the code name package edu.berkeley.icsi.haystack. The Lumen Privacy Monitor application has been installed on both devices used in the study.

c. Application

To test the existence of privacy leaks in the operating system, researchers tested several applications that can cause privacy leaks, there are 5 financial applications tested in this study.

d. Additional File

In addition to the applications mentioned above, there are two files needed for the implementation process in this study, namely files for custom recovery Xiaomi Redmi 4X and Magisk files. The function of custom

recovery is to replace stock recovery that is already installed on a smartphone device, with a custom recovery smartphone device that can be used to install the firmware, rooting, changing file system partitions, making changes, deleting, and adding file system directories, and other software execution commands. Which can only be done at the lowest system level.

While Magisk is a tool needed to provide rooting access to applications running on the operating system. To block leaks and advertisement privacy using the AdAway application requires rooting permission from the Magisk application. The rest Magisk can be used to modify performance, appearance, and certain functionalities in the Android operating system.

3. Data collected

Privacy leaks can be detected using a special application namely Lumen Privacy Monitor, the way it works is by recording and analyzing network traffic transmitted by smartphone devices. The data recorded includes the type of privacy leaks that occur on the device, applications that perform privacy leaks, and overall network traffic data.

Overall this research can be explained in the following flowchart diagram (see the next page):

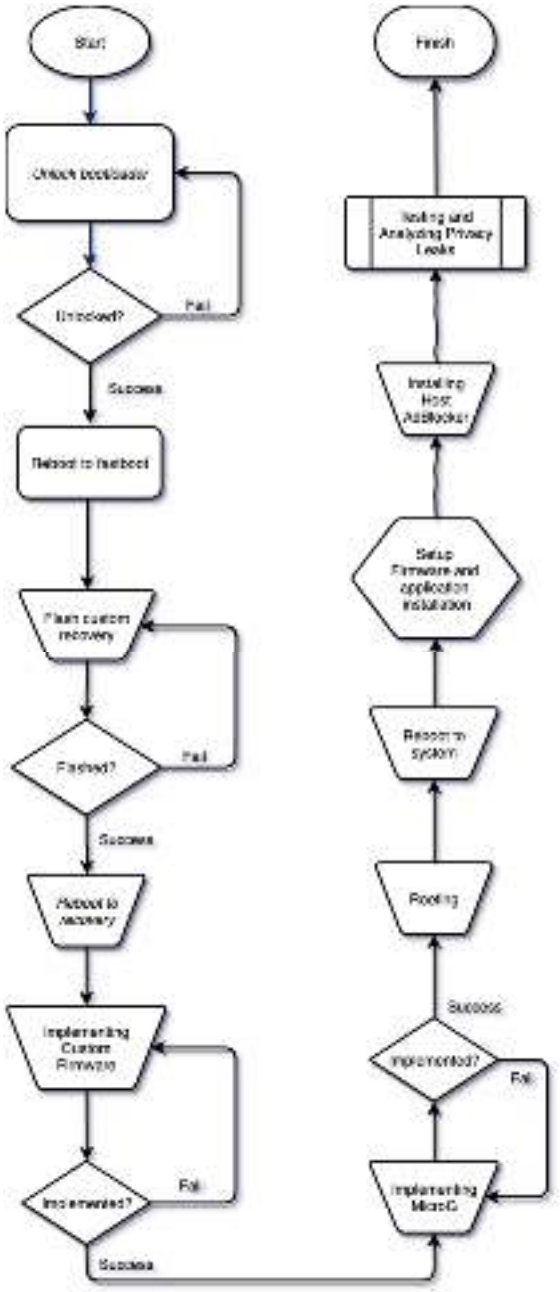

Figure 1. Flowchart diagram of the experimental research process

Once the result of Lumen Privacy Monitor is obtained then the next step is to connect the effect of implementing the libraries to the privacy protection of the device:

This research was conducted to test the existence of privacy leaks on Android devices using the Lumen Privacy Monitor testing method and implemented a solution that can be done to minimize privacy leaks from the user side. The results of the study below answered two research questions filed in the above chapter.

a) There is a privacy leak caused by built-in apps and third-party apps installed on a smartphone

First-stage testing, researchers tested unmodified devices, operating systems that were still original, and their configuration following the initial conditions of the vendor. To increase the value of internal validity, test devices only installed applications that are tested according to the list of applications mentioned in the chapter of the research methodology. The results obtained from the Lumen Privacy Monitor application analysis on unmodified devices are as follows:

1) Type of privacy leak on the device before being protected

Table 1. Privacy leaks types on an unprotected device

No	Leaks type	Value
1	Installed Apps Mid Risk	com.android. providers.downloads
2	Brand Low Risk	Xiaomi
3	Device Model Low Risk	Redmi 4X
4	Build Fingerprint Low Risk	OPM1.171019.026

From the table above, it can be noted that unmodified experimental devices have four types of privacy leaks consisting of one type of privacy leak at medium risk and three types of privacy leaks at low risk. Privacy leak in unprotected devices are; list of apps installed on the device, device brand, device model, and Build Fingerprint.

The privacy leak of installed app listings at risk is due to provide information to other parties about the personality, tastes, and demographics of the information owner. This privacy leak allows advertisers to study demographics and studies for advertising purposes.

In addition to the application list leak, privacy leaks in the form of brands, device models, and build fingerprints are at low risk as this information may be combined with other identifiable information, to make a unique identification of the user.

Applications typically use a variety of information that can be found on the device as a way to adapt the content displayed to fit the device interface and streamline ads. However, this information can be used to identify the user's personality, tastes, wealth, and demographics.

2) Apps that leaking privacy based on Lumen Privacy Monitor

Based on the analysis results of the Lumen Privacy Monitor found that out of the seven applications tested on the device showed that the seven financial digital wallet applications were indicated to collect privacy

data and transmit on a third party server without clear and direct notifications to the user. All third-party applications carry 14 types of privacy Tracker installed in the application's source code.

In addition to the applications tested in this study, Lumen Privacy Monitor also detects that nine built-in applications also perform tracking and advertisement actions on the device. Of the nine devices detected that there are four types of third-party domains that perform tracking on user devices for analysis and advertiser purposes.

3) Analyze Device network traffic based on Lumen Privacy Monitor

Based on the analysis results that Lumen Privacy Monitor does on the network of unprotected devices are found in the following results:

Table 2. Network traffic on an unprotected device

Total connection	312,768
Total unique IP addresses	52,416
Analyzed volume traffic	4320 Mb
Network type	100% WiFi
Ads and Analytic traffic overhead	19 %

From the above results can be noted that the total number of devices carried out as much as 312,768 includes the entire connection made by both built-in applications and third-party applications. There are then 52,416 unique IP addresses that are accessed by the device. The traffic Volume performed by a device by 4,320 megabytes with a 100% network connection is performed on a Wi-Fi network. Lumen Privacy Monitor analyzes that of the total network traffic that the device takes, 19% is used for tracking user activity on the device and the appearance of ads within the device.

From the analysis performed by Lumen Privacy Monitor on unmodified devices found that there is a privacy leak done by third-party applications and built-in applications.

b) There is a decline in the number of privacy leaks on devices that have been protected using custom firmware, MicroG, and Host Adblocker.

The second research is done after the device is modified to improve Android device protection from privacy leak risk. The implementation of the protection is already described in the previous chapter of the research method and the installed applications following the list of tested applications.

To increase the internal validity of the test, this test uses an action dataset that is limited by the access time and actions taken for post-implementation testing equal to pre-implementation testing. The value difference in the Lumen Privacy Monitor test results is used as a benchmark of privacy leaks in the

before and after implementation of device protection.

The following are the results of the Lumen Privacy Monitor test on devices that have been protected:

1) Types of privacy leaks on devices that have been given protection

Table 3. Privacy leaks types on the protected device

No	Leaks type	Value
1	Device Model Low Risk	Redmi 4X
2	Build Fingerprint Low Risk	PQ31.190801.002

From the table above, it is known that the modified experimental device has two types of privacy leaks consisting of two types of privacy leaks at low risk. Privacy leak types include the device model and Build Fingerprint.

Privacy leaks in the form of device models and fingerprint builds are at a low risk as this information may be combined with other identifiable information, to make a unique identification of the user.

Applications typically use a variety of information that can be found on the device as a way to adapt the content displayed to fit the device interface and streamline ads. However, this information can be used to identify the personality, tastes, wealth, and demographics of the user.

By comparing the test results on the device before it is modified, it is known that the number of privacy leak types decreases to two types of privacy leaks, and the risk of privacy leak becomes a low risk.

2) Apps that leak privacy based on Lumen Privacy Monitor on protected devices

Based on the analysis results that Lumen Privacy Monitor has found that out of the seven applications tested on the device indicates that there are five financial digital wallet applications collecting data that are privacy and transmit On a third party server without clear notifications and directly to the user. All third-party applications carry six types of privacy tracker built into the application's source code.

In addition to the applications tested in this study, Lumen Privacy Monitor does not detect built-in apps to perform tracking and privacy leak activities on third parties.

Comparing the test results between protected and unprotected devices gets the result that the number of apps that perform user privacy tracking and the leak has decreased from the original seven applications Indication of a privacy leak, decreasing to five apps that are indicative of privacy leaks.

Besides, the number of third-party domains decreases from 14 domain types to six third-party domain types that are indicative of privacy leaks. Furthermore, the built-in apps on unmodified devices are known to indicate a privacy leak while the modified device has no privacy leaks.

3) Analysis of the modified device's network traffic

Based on the analysis results that Lumen Privacy Monitor has done on the protected network of devices are found in the following results:

Table 4. Network traffic on the protected device

Total connection	243,072
Total unique IP addresses	30,240
Analyzed volume traffic	3,250 MB
Network type	100% WiFi
Ads and Analytic traffic overhead	11%

From the above results can be noted that the total number of devices carried out as much as 243,072 includes the entire connection made by both built-in applications and third-party applications. There are then 30,240 unique IP addresses that are accessed by the device. The traffic Volume performed by a device by 3,250 megabytes with a 100% network connection is performed on a Wi-Fi network. Lumen Privacy Monitor analyzes that of the total network traffic that the device takes, 11% is used for tracking user activity on the device and the appearance of ads within the device.

Comparing with testing on unprotected devices is found the result that with the same traffic volume, the number of connections performed on both devices is different. Unmodified devices have a heavier network load due to third-party tracking activity and advertise. While the modified device has a burden of leakage of privacy and advertisers are smaller than the unprotected devices.

Based on the above comparison can be concluded that there is a decrease of privacy leak on devices that have been modified with Custom Firmware, MicroG, and host Adblocker.

CONCLUSION

Based on the results of experimental research conducted, the following conclusions can be drawn:

1. On unmodified devices, there is still a privacy leak caused by third-party applications and native applications from the vendor.
2. To address the privacy leak issue, researchers file the use of custom firmware, MicroG, and host adblockers that can handle the number of privacy leaks that occur on the device.

BIBLIOGRAPHY

[1] R. C. Basole and J. Karla, “Value Transformation in the Mobile Service Ecosystem: A Study of App Store Emergence and Growth,” *Service Science*, vol. 4, no. 1, pp. 24–41, Mar. 2012, doi: 10.1287/serv.1120.0004.

[2] T. Nguyen, “Mobile Enterprise Applications: Customisation and Distribution,” 2019.

[3] D. Arp, E. Quiring, C. Wressnegger, and K. Rieck, “Privacy threats through

ultrasonic side channels on mobile devices," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2017, pp. 35–47.

[4] G. Russello, B. Crispo, E. Fernandes, and Y. Zhauniarovich, "YAASE: Yet Another Android Security Extension," in *2011 IEEE Third Int\textquotesinglel Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int\textquotesinglel Conference on Social Computing*, 2011, doi: 10.1109/passat/socialcom.2011.151.

[5] Y. Pusparisa, "LinkAja, OVO, atau Go-Pay: Mana yang Anda Pilih?," *Kata Data*, 16-Jul-2019. [Online]. Available: https://katadata.co.id/infografik/2019/07/16/linkaja-ovo-atau-go-pay-mana-yang-anda-pilih.

[6] W. Enck, M. Ongtang, and P. McDaniel, "Understanding Android Security," *IEEE Security & Privacy Magazine*, vol. 7, no. 1, pp. 50–57, Jan. 2009, doi: 10.1109/msp.2009.26.

[7] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions," in *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS \textquotesingle12*, 2012, doi: 10.1145/2335356.2335360.

[8] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These arent the droids you looking for," in *Proceedings of the 18th ACM conference on Computer and communications security - CCS \textquotesingle11*, 2011, doi: 10.1145/2046707.2046780.

[9] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and fine-grained mandatory access control on android for diverse security and privacy policies," in *Presented as part of the 22nd ${$USENIX$}$ Security Symposium (${$USENIX$}$ Security 13)*, 2013, pp. 131–146.

[10] W. Enck *et al.*, "TaintDroid," *Communications of the ACM*, vol. 57, no. 3, pp. 99–106, Mar. 2014, doi: 10.1145/2494522.

[11] M. Zheng, M. Sun, and J. C. S. Lui, "DroidRay," in *Proceedings of the 9th ACM symposium on Information, computer and communications security - ASIA CCS \textquotesingle14*, 2014, doi: 10.1145/2590296.2590313.

[12] J. Huang, O. Schranz, S. Bugiel, and M. Backes, "The art of app compartmentalization: Compiler-based library privilege separation on stock android," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1037–1049.

[13] N. T. Can, P. Van Hau, and N. A. Tuan, "Detect Security Threat In Android Custom Firmware By Analyzing Applications Framework And Default Settings," *PROCEEDING of Publishing House for Science and Technology*, 2019.

[14] H. Meng, V. L. Thing, Y. Cheng, Z. Dai, and L. Zhang, "A survey of Android exploits in the wild," *Computers & Security*, vol. 76, pp. 71–91, 2018.

[15] S.-T. Sun, A. Cuadros, and K. Beznosov, "Android Rooting," in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM \textquotesingle15*, 2015, doi: 10.1145/2808117.2808126.

[16] M. Neeraj, "Android Stock ROM vs Custom ROM: Which One is Better?," *Dazeinfo*, 30-Jan-2020. [Online]. Available: https://dazeinfo.com/2017/04/10/android-stock-rom-custom-rom/.

[17] J. ZHI, C. LIU, and Z. SU, "New Hidden Technology Based on Android," *DEStech Transactions on Computer Science and Engineering*, no. iteee, Mar. 2019, doi: 10.12783/dtcse/iteee2019/28750.

[18] A. Conway, "Unofficial LineageOS Fork with Built-in microG Lets You Avoid Google Services," *XDA*

Developers, 04-Nov-2017. [Online]. Available: https://www.xda-developers.com/unofficial-lineageos-built-in-microg-avoid-google-services/.

[19] G. Kim, "On computing similarity of android executables using text mining," in *Proceedings of the Symposium on Applied Computing - SAC \textquotesingle17*, 2017, doi: 10.1145/3019612.3019926.

[20] G. Merzdovnik *et al.*, "Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2017, doi: 10.1109/eurosp.2017.26.

[21] Singh, "How To Remove Bloatware From Your Xiaomi Device (No Root Required)?," *Fossbytes*, 11-Nov-2019. [Online]. Available: https://fossbytes.com/miui-hidden-settings-for-xiaomi-remove-bloatware/.

[22] India Tech Today, "Here is data Xiaomi records from people who use its phone, and it's almost everything," *India Tech Today*. [Online]. Available: https://www.indiatoday.in/technology/news/story/here-is-data-xiaomi-records-from-people-who-use-its-phone-and-it-s-almost-everything-1226428-2018-05-04.

[23] A. Saxena, "A Secure Dynamic Remote User Authentication without any Secure Channel," in *New Technologies, Mobility and Security*, Springer Netherlands, pp. 617–617.

[24] D'sa, "Is Xiaomi really spying on the your privacy?," *Deccan Chronicle*, 13-Nov-2019. [Online]. Available: https://www.deccanchronicle.com/141023/technology-mobiles-and-tabs/article/xiaomi-really-spying-indian-user%E2%80%99s-privacy.

[25] IndiaTimes, "Xiaomi Sorry for Secretly Mining Data.," *India Times*, 13-Nov-2019. [Online]. Available: https://www.indiatimes.com/technology/enterprise/xiaomi-admits-to-secretly-collecting-user-data-apologises-167385.html.

[26] Sarkar, "New Xiaomi US privacy policy will collect users' personal info, financial details and more," *Gadgets Now*, 04-May-2018. [Online]. Available: https://www.gadgetsnow.com/tech-news/new-xiaomi-us-privacy-policy-will-collect-users-personal-info-financial-details-and-more/articleshow/64026044.cms.

[27] A. Moore, "Defining Privacy," *Journal of Social Philosophy*, vol. 39, no. 3, pp. 411–428, Sep. 2008, doi: 10.1111/j.1467-9833.2008.00433.x.

[28] S. Spiekermann, "Perceived Control," in *Digital privacy: theory, technologies, and practices*, Auerbach Publications, 2017, pp. 267–281.

[29] C. Gibler, J. Crussell, J. Erickson, and H. Chen, "AndroidLeaks: Automatically Detecting Potential Privacy Leaks in Android Applications on a Large Scale," in *Trust and Trustworthy Computing*, Springer Berlin Heidelberg, 2012, pp. 291–307.

[30] L. Li, A. Bartel, J. Klein, and Y. Le Traon, "Detecting privacy leaks in Android Apps," 2014.

[31] J. I. Kim, H. S. Yoon, G. Yi, H. S. Kim, W. Yih, and W. Shin, "The Plastid Genome of the Cryptomonad Teleaulax amphioxeia," *PLOS ONE*, vol. 10, no. 6, p. e0129284, Jun. 2015, doi: 10.1371/journal.pone.0129284.

[32] R. Slavin *et al.*, "Toward a framework for detecting privacy policy violations in android application code," in *Proceedings of the 38th International Conference on Software Engineering - ICSE \textquotesingle16*, 2016, doi: 10.1145/2884781.2884855.

[33] M. M. Orozco, "College of Computer Studies Graduate Tracer with Data Analytics," in *Abstract Proceedings International Scholars Conference*, 2018, vol. 6, pp. 220–220.

[34] A. Razaghpanah *et al.*, "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem," in *Proceedings 2018*

Network and Distributed System Security Symposium, 2018, doi: 10.14722/ndss.2018.23353.