# MULTIPLE FLAWS IN XIAOMI'S MIUI SYSTEM APPS INTRODUCE UN-INTENTIONAL VULNERABILITIES INTO END-USER APPS AND SECURITY APPS

A comparative study, between Xiaomi's MIUI System Apps and various Security/Backup-restore apps, vis-à-vis the functional working of the end-user apps and the security controls implemented by them.

## ABSTRACT

During our initial tests, we realized that Xiaomi's Uninstall feature introduces an unintentional bug in the implementations of Third-Party Security Apps developed for Android. Furthermore, MI-Mover can access App-System-Data which allows cloning of the End-User apps. Hence, it was necessary to analyse the behaviour of all the Security Apps and backup/restore apps along with the behaviour of end-user apps w.r.t. the implementation of the security controls and the overall impact was needed to be analysed.

| | |
|---|---|
| **Research by : Sachin Raste** | **Organization : eScan** |
| **Sr. Research Analyst** | **www.escanav.com** |
| **Contact : sachinr@escanav.com , Twitter : @essachin** | |

# TABLE OF CONTENTS


| | TOPICS | PAGE NO. |
|---|---|---|
| **1.** | DISCLAIMER | 3 |
| **2.** | INTRODUCTION | 4 |
| **3.** | SECURITY APPS / ANDROID FOR WORKS AND THE UN-INSTALL FEATURE | 6 |
| **4.** | GRADING OF APPS AND BASIC FUNDAMENTALS OF INFORMATION SECURITY | 9 |
| **5.** | TESTING SCENARIOS | 9 |
| **6.** | INSTALLATION AND DEVICE REGISTRATIONS | 10 |
| **7.** | LIST OF BACKUP AND RESTORE APPLICATIONS TESTED | 11 |
| **8.** | LIST OF END-USER APPLICATIONS TESTED DURING BACKUP AND RESTORE | 12 |
| **9.** | TESTING, ANALYSIS AND GRADING OF BACKUP/RESTORE APPS | |
| | A. THIRD PARTY APPS | 14 |
| | B. DEVICE MANUFACTURER DEVELOPED APPS | 14 |
| **10.** | TESTING, ANALYSIS AND GRADING OF END-USER APPS | |
| | A. TRAVEL | 16 |
| | B. WALLETS | 18 |
| | C. SOCIAL NETWORKING | 20 |
| | D. TRANSPORTATION | 24 |
| | E. SHOPPING | 27 |
| | F. SECURE DOCUMENTS | 29 |
| **11.** | CONCLUSION AND REMEDIATION | 30 |
| **12.** | APPENDIX A – POC | 33 |
| **13.** | APPENDIX B – VENDOR RESPONSE | 34 |
| **14.** | APPENDIX C – ANDROID SANDBOX MODEL | 35 |
| **15.** | APPENDIX D – REFERENCES | 36 |

## DISCLAIMER

Due to the very nature of the multiple flaws which affect the functional working of Third-Party-Apps, we tested only a few of the apps from each of the categories mentioned in this report, due to the existence of many apps and testing every app was not humanly possible. Exclusion of any app doesn't signify that these apps or categories are not affected by these flaws nor is it related in any way to the popularity. It is the responsibility of individuals and app developers alike to test the apps and act in favour of ensuring that their users/data are protected.

We tested a few of the banking apps and after being notified they have taken cognizance of the mentioned issues. Furthermore, some of them have issued out of turn patches too. However, we have decided to withhold the names and shall conduct testing of banking apps with an additional set of parameters.

The app developers were contacted using every possible method and ample of time was provided for them to decide on the issues outlined in this report.

# INTRODUCTION

Privacy is the gravest concern of all, and in today's interconnected world, there is a very thin line between our personal lives, our data, and the Internet. Numerous countries have laws pertaining to Privacy and Breach of Privacy, with the toughest being the Safe Harbor Law of the EU. However, the foremost question which can be raised is that whether laws actually protect the privacy or is it simply deterrent for app developers, who may digress away from laying down norms?

Mobile device manufacturing market is highly vibrant and competitive, newer devices/phones with more advanced features are making foray into our daily lives, statistics are being collected, however, what type of data is being collected under the garb of statistics is not well documented by any of the manufacturers or by the application developers, and this aspect is not covered in the research.

This research specifically looked into the apps developed by manufacturers or by third-party, which would provide end-users with the capability to protect their devices i.e. Security and backup/restore apps. Did any of the apps violate the basic principles of Information Security? It is to be noted that these same principles are adhered to by the app developers and sometimes these apps /app developers get reprimanded for their over-sight and putting to risk the end-user's identity and data.

Moreover, when the apps contravene the set standards/guidelines, Privacy isn't the only aspect which gets affected; we face other issues viz. Repudiation, Identity-Theft or Impersonation and Corporate IT Security.

The Research is segregated into multiple parts, as mentioned below:

Part 1 of the Research

1. Un-Installation procedure followed by various Third-Party Device Security Apps.
2. Removal of Android for Works Admin Apps.

Part 2 of the Research

3. In-built security processes for user/device registration.
4. Verification of the devices / users at the time of use.

Part 3 of the Research

5. Content which is transferred during Backup/Restore.
6. Behaviour of apps before and after Restore.

# SECURITY APPS / ANDROID FOR WORKS

# AND

# THE UNINSTALL/REMOVAL FEATURE

## REMOVAL OF SECURITY APPS

Smartphones provide device security in form of Pattern or Password Lock and in some cases Fingerprint Lock when available. Android based smartphones although provides security at the lock-screen itself. Anti-Theft Apps for these devices provide an additional layer of security to the devices and provide various features related to remote lock/wipe, uninstall protection etc. These apps at the time of install require the permission for being a Device Administrator and are protected by a password so as to ensure that any unauthorized person is unable to un-install them.

Contrary to the common belief that pattern/password lock should suffice and would pose a significant level of difficulty to any person trying to gain access to the device, the Anti-Theft apps provide authenticated mechanism to prevent removal of itself from the device. Generic steps to uninstall/remove would require the user to disable admin privilege for the app first and then provide the valid Authentication to remove the app entirely from the device.

MIUI's system app which handles the un-installation of the apps, it poses a significant threat to Security apps. It has been observed that these apps at the time of un-install would ask for a password on all the devices, although on MIUI, these apps get un-installed without the need for a password. From a security point of view, the process of un-install implemented in MIUI poses a significant security threat since the authentication process implemented by the app is bypassed.

End-Users have always felt comfortable with the fact that their device is protected by an additional layer and the very purpose of implementing this feature by security apps is defeated. The device owners of MIUI will now have to solely rely on the pattern/passcode lock provided by the MIUI, moreover, they will have to ensure that they do not enable Smart-Lock which is an inherent feature.

Since all the Security Apps installed on MIUI were affected by this design flaw; hence we do not find it necessary to provide additional details.

Advisory: For Security App Developers

1. Every Security App developer should test their apps afresh on Xiaomi Devices.

## REMOVAL OF ANDROID FOR WORKS ADMIN APPS

Android has moved into the Enterprise space with it Android for Work, which is a welcome relief to all the working professionals who have to juggle with multiple devices. Android for Work provides segregation of workspaces and profiles within the same UI and the Apps are aptly differentiated by a visible red-briefcase badge attached to the Work-Profile related Apps.

It provides an easy way of administration for the IT personnel with the ability to install/remove work related apps and moreover they can even remote wipe the entire Work-Space without gaining access to the personal space of the Device Owner on the Device.

According to Google, on Android 5.0+ devices, you can delete your work profile in Settings > Accounts > Remove work profile. Touch Delete to confirm the removal of all apps and data within the work profile.

After the work profile is deleted, all local data on the device within that profile is deleted. Only the device policy controller application and the Android device owner can delete the work profile and data. However, only the owner of the device can delete the personal data and perform a factory data reset. If a device is owned by your company or organization and configured with a device owner, the device owner can also perform a factory reset.

MIUI inefficiently handles removal of workspace related to Apps designed to facilitate Android for Works. Furthermore, due to the fact that in MIUI, the Workspace Profiles aren't properly labeled it becomes all the more difficult to differentiate between Personal and Work Profiles.

Removing of Work-Profile Admin App has a negative impact on the functional working/implementation of Android For Works Apps and it defeats the very purpose of implementing Android for Works on Xiaomi Devices.

Advisory: For Android for Work App

1. App Developer organizations should test their apps afresh on Xiaomi Devices.
2. Organizations implementing Android for work should evaluate the solution for these devices too.

Unless and until Xiaomi takes stringent steps to properly implement Android for Works, Organizations should exercise caution while developing / implementing EMM solutions for/on these devices.

# END-USER APPS AND MI-MOVER

## GRADING OF APPS AND BASIC FUNDAMENTALS OF INFORMATION SECURITY

While designing an App or Software, implementing security controls is now treated as a part of the design stage. The research emphasized on the CIA Triad i.e. Confidentiality, Integrity and Availability, coupled with Access Control which is related to Identification, Authentication, Authorization and Accounting. It is assumed that all the Apps were developed/designed based on the sensitivity of data and that they adhered to these ideologies in some form or the other.

The grading of the Apps in this research is based on the very fundamentals which constitute Information Security. It is to be noted that every app has a different set of security controls and mechanisms since all of these apps do not fall under the same category and the required levels of Security Controls differ, however, apps from the same category have to implement similar levels of security mechanisms and controls. The level of Impact which ultimately affects the Identification, Authentication and Authorization mechanisms implemented vis-à-vis the Confidentiality and Integrity levels required for smooth functioning/implementation of these controls for the particular category of businesses are also considered an important aspect for grading.

## TESTING SCENARIOS

| App | Devices | Device A | Device B | Device C |
|---|---|---|---|---|
| **Xiaomi MI-Mover** | 3 | Yureka (Yu) | Xiaomi Model 1 (Mi-1) | Xiaomi Model 2 (Mi-2) |
| | Backup / Restore between Yureka and any of the Xiaomi Devices. – Installed MI-Mover from Playstore on Yureka YU, then initiated the backup/restore and vice-versa<br>Backup / Restore between Xiaomi Model 1 and Xiaomi Model 2. – Used the MI-Mover system app then initiated backup/restore | | | |
| | | | | |
| **Samsung Smart-Switch** | 3 | Yureka (Yu) | Samsung Galaxy Model 1 (SG-M1) | Samsung Galaxy Model 2 (SG-M2) |
| | Backup / Restore between Yureka and any of the Samsung Devices. – Installed Smart Switch from Playstore on Yureka YU, then initiated the backup/restore and vice-versa<br>Backup / Restore between Samsung Model 1 and Samsung Model 2. – Used the Samsung app then initiated backup/restore | | | |

| Scenario 1 (S1) | Scenario 2 (S2) | Scenario 3 (S3) | Scenario 4 (S4) |
|---|---|---|---|
| **Yu <-> M1-n** | **Mi-1 <-> Mi-2** | **Yu <-> SG-M1** | **SG-M1 <-> SG-M2** |

Mi-Mover on Xiaomi devices can be started by accessing **SETTINGS → ADDITIONAL SETTINGS → MI MOVER** or by downloading and installing it from Google Play while using a non Xiaomi Phone. The sender and receiver both have to start Mi-Mover, by selecting the appropriate option related to Sender/receiver, while the sender has to share the QR Code with the Receiver. All the other apps mentioned in here have to be downloaded from Play Store or from their respective manufacturer's app store, e.g. Samsung Smart Switch can be downloaded from Samsung Tools store.

## INSTALLATION AND DEVICE REGISTRATIONS

End-User Apps belonging to various categories have different levels of implementation of managing App Security. A Banking App would be more secure in comparison to a Travel / Transportation App which would have different levels of security verifications inbuilt at the time of Installation and during its usage under normal circumstances.

When we look into various processes, which are part of the user's transaction, then these can be segregated into various components and the implementation of security at various stages has to be analysed. There are some apps which permit persistent logins due to which, credentials are not required whenever the app has been launched. Hence we flag such applications at "Low level" as any unauthorized person may gain access to some of the sensitive areas of the applications. Owing to this we immediately shift our focus to these areas - whether access to these areas is restricted or not. Based on the combination of these factors the overall severity impact level is decided.

App requesting the user to provide access credentials every time they are launched should be considered secure up to a certain extent since any person wanting to gain unlawful access would have to first initiate phishing attack before gaining physical access to the phone.

Some of the Wallet app developers are of the view that, end-users regularly use their app and launched every other minute. However, when we compare the usage pattern, Social Networking Apps are way ahead in usage, hence requesting a user to provide their password / Passcode / MPIN every time a Social App is opened would be cumbersome, however all the apps which provide Wallets or App Security, should understand that security of the end-user data and their credentials are of prime importance and any feature which protects the information shouldn't be optional.

Session Time-out is an often overlooked security feature and during the testing of Security based SAAS product, we came across a product which will not terminate the present session, no matter how much time you have been inactive. However, the vendor's other SAAS product didn't have such issues; the session is terminated after two to three minutes of inactivity.

Mobile Apps and its usage has a very different perspective, and for some unknown reasons, irrespective of the sensitivity of the information handled by the app, many of the apps do not provide the auto-lock /session termination, but they would provide a logout, which in any case is entirely useless since we have rarely seen users using the logout. When using Desktops / Laptops, the same user would logout or the session might get timed-out. However, it's quite the opposite when the same user accesses the same website from Smartphone. This also holds true for Apps too and the majority of the Apps do provide logout feature which the users rarely use.

# LIST OF BACKUP AND RESTORE APPLICATIONS TESTED

| Category | Apps | Manufacturer | Description |
|---|---|---|---|
| Third-Party Backup/Restore Apps | Xender | Third-Party | Xender is a file sharing & transferring application between mobile devices, either Android or iOS based, with no need for cables or Wi-Fi or cellular Internet connection. More than 80 million activated users globally, Xender also covers all time zones and published in more than 30 different languages |
| | ShareIT | Third-Party | The world's preferred app for cross platform sharing 200 times faster than Bluetooth and choice of 1 billion people. Users can share with friends as well as transfer their personal content on the go, between all of their devices at rapid speed |
| | Titanium Backup | Third-Party | Requires Root for 100% app data transfer |
| | Helium | Third-Party | Requires Root for 100% app data transfer |
| Device Manufacturer Developed Backup/Restore Apps | SmartSwitch | Samsung | Samsung's SmartSwitch helps you in syncing your data and accounts between Samsung phones |
| | MI Mover | Xiaomi | Xiaomi's Mi Mover helps you move your apps and data from an old Non-MI or MI device to a Mi Phone. Transfer contacts, messages, photos, music, videos, documents, installed apps, and other data air two devices using a QR code and start transferring instantly. Connection speed up to 6MB/s, even faster than restoring data from cloud backup, mobile data, or Internet required |

# LIST OF END-USER APPLICATIONS TESTED DURING BACKUP AND RESTORE

| Category | End-User App | Description |
|---|---|---|
| Travel | Goibibo | Goibibo is the largest online hotels booking engine in India and also one of the leading air aggregator. Other than that users also can book Train, Bus & Cars online through the app |
| | Yatra | A strong and "trusted" travel and multi-channel platform for leisure and business travellers, a robust mobile eco-system for a spectrum of travellers and suppliers all over India and abroad. Since the inception in 2006, more than 4 million users with over 61,000 hotels contracted in over 1,100 cities across India |
| | MakeMyTrip | MakeMyTrip has revolutionized the travel industry over the years. One of India's Online Travel Leader founded in the year 2000 by Deep Kalra. Created to empower the Indian traveller with instant booking and comprehensive choices |
| | Airbnb | Airbnb is a trusted community marketplace for people to list, discover, and book unique accommodations around the world. Airbnb connects people to unique travel experiences, at any price point, in more than 65,000 cities and 191 countries. And with world-class customer service and a growing community of users |
| | IRCTC | IRCTC app has been set up by the Ministry of Railways with the basic purpose of the New Users, register from App directly, Search and Book train tickets, View and Cancel tickets Current reservation & Boarding point change facility |
| | | |
| Wallets | PayTM | PayTM is India's largest mobile payments and commerce platform. It started with online mobile recharge and bill payments and has an online marketplace today. In a short span of time grown to over 220 Mn registered users. PayTM is the consumer brand of India's leading mobile internet company One97 Communications. One97 investors include Ant Financial (AliPay), SAIF Partners, Mediatek, Sapphire Venture and Silicon Valley Bank |
| | JioMoney | JioMoney is recent ecommerce platform in the e-wallet market started by Reliance Payment Solutions Ltd. This apps feature enables its users can pay utility bills, Cash back offers, other offers and deals, pay for ticket bookings etc. also one can transfer money digitally through the app |

| Category | End-User App | Description |
|---|---|---|
| Social | WhatsApp | WhatsApp Messenger is a cross-platform instant messaging application that allows iPhone, BlackBerry, Android, Windows Phone and Nokia Smartphone users to exchange text, image, video and audio messages for free |
| | Facebook | Facebook is a social networking website and service where users can post comments, share photographs and links to news or other interesting content on the Web, play games, chat live, and even stream live video. Shared content can be made publicly accessible, or it can be shared only among a select group of friends or family, or with a single person |
| | Facebook Messenger | Facebook Messenger is an instant messaging service and software application. It is integrated with Facebook's web-based chat feature and built on the open MQTT protocol. Facebook Messenger lets Facebook users send messages to each other |
| | Twitter | Micro-blogging and limits the tweets to 140 characters |
| | Telegram | Telegram is a free cloud instant messaging service. Telegram clients exist for both mobile (Android, iOS, Windows Phone, Ubuntu Touch) and desktop systems (Windows, Mac-OS, Linux). Users can send messages and exchange photos, videos, stickers, audio, and files of any type. Telegram also provides optional end-to-end-encrypted messaging |
| | | |
| Transportation | Uber | Uber is a 24*7 cab service app used for hiring or sharing the rides |
| | OLA | Ola is a 24*7 cab service app where you can hire or share your ride to travel with easy payment options of cash and e – wallet |
| | | |
| Shopping | Amazon | Amazon is the largest online shopping app dealing with Electronics, Books, Kitchenware, Appliances, Health & Personal care, Apparel, Sports, Shoes, Jewellery , Furniture and more |
| | Amazon Prime Video | Amazon Prime provides Movies, TV Shows for Online Viewing |
| | Flipkart | Flipkart is an online shopping app which has products in Fashion, Electronics, Books, Mobiles and other categories |
| | SnapDeal | SnapDeal is the online shopping app for clothing, fashion, electronics, home & kitchen essentials, gadgets, mobile recharge, booking cabs, ordering food and more |
| | | |
| Secure Documents | DigiLocker | DigiLocker is a platform for issuance and verification of documents & certificates in a digital way, thus eliminating the use of physical documents |

# TESTING, ANALYSIS AND GRADING OF BACKUP/RESTORE APPS

1. THIRD PARTY APPS

These popular Backup and Restore apps allows users to share between their devices

a. APKs
b. Non-System Data on non-rooted phones viz. documents, images, directories

However, these applications do not provide access to the system directories where most of the apps store the information related to account access and other sensitive data.

During Installation, of Xender or ShareIT, Access Credentials are not created nor is there any type of Two Factor Authentication (TFA) or binding with the Phone's PIN/Pattern lock available when File/App transfer is initiated, due to which these two apps are vulnerable to data pilferage whenever someone has physical access to the phone by unfair means .

Since APKs are transferred and have to be manually installed, any App specific data which resides in the app-system-storage area is not accessed by these Third-party Backup apps; hence the registration and other sensitive information don't get copied into the new device. Although, the app specific data residing in user-space was copied into the new device and re-registration was required.

Severity Impact: High
Advisory:

- For App Developers :
  a. Implement TFA or Integrate Phone's PIN/Pattern/ MPin before initiating any backup procedure.
- For End-Users :
  a. Implement Phone's pattern lock / pin / passphrase, however this is not going to ensure that the app is protected.
  b. Implement Application Locker

2. DEVICE MANUFACTURER DEVELOPED BACKUP/RESTORE APPS

Some of the Device Manufacturers in order to enhance their sales provide their in-house developed apps for backup and restore or when the two devices are from the same manufacturer then system backup/restore apps have higher privileges than those of the third party apps or similar apps are also made available in Playstore by the manufacturers.

Manufacturer developed apps, do have access to the user space but there is a possibility that can also access the app-system-storage areas where app-related sensitive data resides, which under normal circumstances is available only for “rooted” devices. Xiaomi’s MI Mover can be termed as System App and Samsung’s SmartSwitch is available for download from Galaxy App Store hence it is a Manufacturer Developed App. These two are Manufacturer Developed Apps assist the users to sync their devices. Although, both of these apps do not provide basic security viz. restricted access to initiate the transfer, however they do provide the users with the ability to choose the apps, images, videos, documents etc. to be migrated from one device to another. It is to be noted that Samsung’s SmartSwitch allows the users to sync installed apps; however it does not transfer the sensitive data from the system areas, hence, the users of Samsung’s SmartSwitch have to reinitiate the registration process all over again.

Xiaomi’s MI-Mover, on the other hand, transfers all of the system data to the other Xiaomi Device. It is to be noted that this feature is 100% functional when both the devices are manufactured by Xiaomi. From our point of view although this is great feature, however considering the fact that most of the apps used by the users have access to / store sensitive information and moreover these apps at the time of registration, implement various security features to ensure that their apps are being installed and used by Authorized Users, hence it becomes all the more important for us to analyse the Installation, pre-backup, and post restore process of these user apps which would assist us in arriving at the conclusion whether - MI Mover System app is a security hazard and renders the Xiaomi devices vulnerable to data pilferage or is MI Mover the much-needed app for enhancing user experience.

Developers of End-User Apps, implement different processes to ensure the authenticity of their users and also to positively identify the devices. How would these apps behave when the base device changes but the data from an app-system-storage area of the old-device is made available in the new device.

1. Do these third party end-user apps verify the device and then compare it with the values stored in their database?
2. What happens when such verification is not present?
3. Would the app behave as if nothing has changed?
4. What would happen when the same app with same credentials is running from two different non-rooted devices?
5. Would this lead to impersonation and subsequent repudiation of the acts committed?

In order to verify and put to rest all the doubts we have to understand the Registration and Pre-Backup security-specific process of apps and then compare them with the Post-Restore on different non-rooted devices, based on the Test Scenarios explained earlier.

Data Sync between two rooted device would result in 100% replication especially of the app-system-storage, however from holistic point of view, rooting of devices itself is a tedious and time-consuming task and the End-User would be wary of the tasks happening hence, in this research rooted devices and its effect on the apps hasn’t been considered. Moreover, when System-Apps start providing unhindered access to these system areas and allowing unrestricted backup and restore then, it makes the task of stealing and gaining unauthorized access all the more easy. **Hence, for this reason, the Post Restore section concentrates ONLY ON “Xiaomi to Xiaomi” Device App Transfer as all other test scenarios have failed.**

# TESTING, ANALYSIS AND GRADING OF END-USER APPS

## CATEGORY: TRAVEL - PRE BACKUP

All the tested Travel apps require Mobile No or Facebook Authorized Access for allowing the users to utilize the apps, They also provide a wallet for their reward points, moreover credit / debit cards can be saved within the app, however at the time of bookings or accessing the wallet, TFA is not implemented. The only exception was IRCTC, which requested access credentials every time the app was launched.

Advisory:

- For App Developers :
  a. Implement TFA or Integrate Phone's PIN/Pattern/ MPin before allowing access to Wallet or initiating any transaction.
- For End-Users :
  a. Implement App Locker

| App | Registration | OAuth | During Launch | Wallet | During Payment | Severity Impact |
|---|---|---|---|---|---|---|
| **Goibibo** | Mobile + Password + email | Facebook | Not Asked. (access credentials required for new installs or after in-app logout) | Yes. Card Details Saved | No TFA | Medium |
| **Yatra** | Mobile + Password + email | Facebook | Not Asked. (access credentials required for new installs or after in-app logout) | Yes. Card Details Saved | No TFA | Medium |
| **MakeMyTrip** | Mobile + Password + email | Facebook Google | Not Asked. (access credentials required for new installs or after in-app logout) | Yes. Card Details Saved | No TFA | Medium |
| **Airbnb** | Mobile + Password + email | Facebook , Google, Weibo | Not Asked. (access credentials required for new installs or after in-app logout) | Yes. | No TFA | Medium |
| **IRCTC** | Mobile + Password + MPIN | No. | MPIN. Stored locally. | Yes. | Pin is required for every booking | None |

## CATEGORY: TRAVEL - POST RESTORE – S2 (BETWEEN TWO XIAOMI DEVICES)

When two Xiaomi devices were used, all the applications allowed the user to log into the app and allowed access to all the history, wallets and conducted operations as if both the devices are same, except for IRCTC App which asked for registration.

Since credentials are cached and the cache itself is being copied from the app-system-storage area, it is imperative for the Apps to at the least implement Device Verification at every launch, so as to ensure that whenever the app detects a change of device. It wipes out the app-related sensitive data and initiates re-registration process. Alternatively, apps could also ask for access credentials and to ensure non-repudiation they should provide an authenticated method to access the interface for the End-User to view all the existing sessions and allow them to terminate the session. However, in these apps Audit Trail, Access Logs do not exist. Although, the impact of the severity is High, due to the fact that these apps constantly keep on sending reminders the end-user would know that something is wrong and would alert, hence the impact severity has been downgraded to Medium.

Advisory for App Developers:

a. Device Verification at every Launch.
b. Auto Lock Sessions, Authenticated Session termination.
c. When Device change detected at least ask for Access Credentials.
d. Audit Trail of Access and Login Notification.

| App | Registration/Launch Access restrictions | Credentials State | Login Access Notification | Session Termination | Severity Impact |
|---|---|---|---|---|---|
| **Goibibo** | Credentials not asked. Launched with full privileges. | Cached | None | Not Available | Medium |
| **Yatra** | Credentials not asked. Launched with full privileges. | Cached | None | Not Available | Medium |
| **MakeMyTrip** | Credentials not asked. Launched with full privileges. | Cached | None | Not Available | Medium |
| **Airbnb** | Credentials not asked. Launched with full privileges. | Cached | None | Not Available | Medium |
| **IRCTC** | Credentials Required. | MPin cached | None | Not Available | Low |

SCENARIOS TESTED FOR ACCESS OF APP-SYSTEM STORAGE BY OTHER APPS

| | Yu <-> M1-n | Mi-1 <-> Mi-2 | Yu <-> SG-M1 | SG-M1 <-> SG-M2 |
|---|---|---|---|---|
| **Goibibo** | No Access | Access Granted– Affected | No Access | No Access |
| **Yatra** | No Access | Access Granted – Affected | No Access | No Access |
| **MakeMyTrip** | No Access | Access Granted – Affected | No Access | No Access |
| **Airbnb** | No Access | Access Granted – Affected | No Access | No Access |
| **IRCTC** | No Access | Access Granted – Affected | No Access | No Access |

## CATEGORY: WALLETS - PRE BACKUP

All the apps which were tested required a different set of information to complete the registration process, Wallets viz. PayTM and JioMoney needed the mobile no., email-id. Except for PayTM, all of the other tested apps required the end-user to provide their credentials in some form or the other. Since PayTM's implementation is optional, it becomes all the more imperative to look into this app a bit more closely. While making payments, PayTM would either prompt for enabling Patter/Passcode of the phone and while refilling the wallet it doesn't ask for any, considering the fact that it allows the users to save their cards. There are few other factors which govern the over security factor of PayTM's app, due to which it has been awarded a "Low" Severity rating.

Advisory:

- For App Developers :
  a. Security is not optional, it's mandatory. Enforce Pattern / Passcode.
  b. Implement Auto-Lock or Session Timeout.
- For End-Users :
  a. Implement App Locker.

| App | Registration | OTP | TFA | During Launch | Access Wallet / Cards | During Payment / Refill | Severity Impact |
|---|---|---|---|---|---|---|---|
| **PayTM** | Mobile No. email-id, password | Mobile OTP | Pattern / Passcode | None | Pattern / Passcode. Cards Saved | Not Asked | Low |
| **JioMoney** | Mobile No, MPin | Mobile OTP | MPin | MPin | No TFA Asked. Cards Saved | No | None |

## CATEGORY: WALLETS - POST RESTORE- S2 (BETWEEN TWO XIAOMI DEVICES)

Wallets Apps, due to their various security features are a bit complex to analyse, due to this reason every app has been compared with itself for the registration and verification process, and then some generic guidelines were used as a benchmark.

PayTM app, under normal circumstances never asked for credentials at the time of launch, due to this, when it is moved from one device to another using MI Mover, there is no change in the basic functionality, i.e. After launch one can access the wallet, passbook, the saved cards etc. However, very recently PayTM added TFA i.e. The end-user has to enable Device Security Authentication (DSA) on their Devices and this method of authentication was used by PayTM, and when the TFA enabled PayTM app is transferred to the second device which doesn't have any DSA enabled, only the notification is displayed but the user is allowed to view wallet and transfer the monies. It doesn't matter whether DSA is enabled or not on the second device because PayTM will always try to verify using the DSA rather than trying to verify the device or verifying the stored credentials on the server.

It seems, PayTM has tried to patch the need for TFA with a work-around solution rather than implementing a better authentication mechanism, moreover this method of authentication verification should be used in conjunction with some other form of validation/verification. However the second verification should be that of the actual device / or from the server, rather than comparing the credentials stored in the app-system-storage.

Advisory:

- For App Developers :
  a. Device Verification at every Launch.
  b. When Device change detected at least ask for Access Credentials or reinitiate the registration process.
  c. Enforce Server-side verification of MPin / Passcode.
  d. Device Security Authentication coupled with second type of verification/validation.
  e. Auto Lock Sessions and Authenticated Session termination.
  f. Audit Trail of Access and Login Notification.

JioMoney App, require the user to provide their access credentials at the launch of the app hence, these two apps are not affected by the vulnerability introduced by MI-Mover.

| App | Registration/Launch Access restrictions | Credential State | Device Validation | Online Payment | Availability of Session Termination | Severity Impact |
|---|---|---|---|---|---|---|
| **PayTM** | Credentials not asked. Launched with full privileges | Cached | None | Notification for enabling Pattern but allowed to transfer. | No | High |
| **JioMoney** | Requires Username/Password / MPin | Not Cached | By Design | Allowed after Login | No | None |

SCENARIOS TESTED FOR ACCESS OF APP-SYSTEM STORAGE BY OTHER APPS

| | Yu <-> M1-n | Mi-1 <-> Mi-2 | Yu <-> SG-M1 | SG-M1 <-> SG-M2 |
|---|---|---|---|---|
| **PayTM** | No Access | Access Granted– Affected | No Access | No Access |
| **JioMoney** | No Access | Access Granted –Not Affected | No Access | No Access |

# CATEGORY: SOCIAL NETWORKING APPS – PRE BACKUP

Social Networking apps have the highest usage amongst the users, hence the security features offered by these apps and their functional workings were tested.

Although, App Passcode is optional for both WhatsApp and Telegram, however, Telegram has a Cloud Password when enabled would ask for the Cloud Password whenever Telegram is installed on a new device, however with WhatsApp, things seem a bit different, the Passcode in Two-Factor Authentication is randomly asked when the app is launched. Hence, WhatsApp has been awarded a "Low" severity rating. Facebook and Facebook Messenger, provide persistent login with logout, however, except for Telegram none of the tested Messaging apps had Auto-Lock which would lock the app when inactive for certain period of time, due to this the perspective towards the "Always Available" ideology changes and the paradigm shifts towards user privacy. The only problem with Twitter is that the activity logs, of all the logged-in sessions, are not provided.

Advisory:

- For App Developers :
  a. Implement Auto-Lock or Session Timeout.
- For End-Users :
  a. Implement App Locker.

| App | Registration | Install | During Launch | Session Termination | Severity Impact |
|---|---|---|---|---|---|
| **WhatsApp** | Mobile No. MPin | Optional MPin will be asked | Randomly asked | Yes, all WhatsApp Web Sessions can be terminated | Low |
| **Telegram** | Mobile No, Passcode, Cloud Password | Optional Cloud Install Password | Optional Passcode If enabled. | Yes, forcibly all the sessions can be terminated | None |
| **Facebook** | Email-id or mobile no. and password | Access Credentials are required | Never, Persistent Login Session Maintained | Yes, forcibly all the sessions can be terminated | Low |
| **Facebook Messenger** | Email-id or mobile no. and password | If Facebook is installed then access credentials are not asked/ | Never, Persistent Login Session Maintained | Yes, forcibly all the sessions can be terminated | Low |
| **Twitter** | Email, | If mobile no. enabled then OTP is sent | Never | No | Low |

## CATEGORY: SOCIAL NETWORKING APPS – POST RESTORE- S2 (BETWEEN TWO XIAOMI DEVICES)

WhatsApp and Telegram are two of the most popular chat messengers and both of them follow the same methods for registration i.e. Mobile Number + OTP, however, both of them differ by miles when it is related to the implementation of security related features viz. Install Password, App Password and Session Timeout and Management.

It seems WhatsApp has been closely following the implementation of features provided by Telegram, and very recently WhatsApp implemented Two-Step Verification Pin which will be asked whenever WhatsApp is installed on a new phone and this same Pin pops up randomly at least once a day while launching.

WhatsApp allows the users to access WhatsApp from Web-Browser, but it doesn't allow more than one simultaneous browser connections, the rest of the connections are disabled prompting the user either to logout or to resume. This effectively means that at any given point of time One Mobile Device and One Browser Session would be active. When WhatsApp is installed on a second phone, then the WhatsApp on the first phone is disabled.

However, when we use MI-Mover to backup and restore WhatsApp between two Xiaomi Devices, WhatsApp functions normally on both the devices, their encryption keys are the same, while the second offending device is not shown in the Sessions List. Both the devices can communicate with any user in the list, however, the issue is that simultaneous chat has some weird effect on the communications and sometimes the messages are lost. However, when one device is not using WhatsApp, then the Second device can communicate effectively with the groups and others in the list and vice-versa. All the chat contents are never shown on the First Device. To make the matters worse, the two devices are never shown in the Session List; hence the user would never know who else is using the same WhatsApp on their Xiaomi Phone.

Advisory: WhatsApp

- For App Developers :
  a. Device Verification at every Launch.
  b. When Device change is detected initiate re-registration process.
  c. Implement Passcode Lock
  d. Proper handling of Session Identities and its termination.

Telegram is no better than WhatsApp, however, both devices can communicate with the users with ease; the messages are not lost – unless deleted by the users. Additionally, Telegram does provide a session list; however only one device is shown in it and terminating the session would terminate all the sessions which have been cloned. Due to this, the session on both the Devices gets terminated and Telegram initiates the Registration Process.

Moreover, Telegram has provided Passcode Lock and Two-Step Verification. Passcode lock when enabled would lock the App based on the time-out provided, while Two-Step Verification is related to Installation password. Due to the fact that Telegram can be installed on multiple devices / OSes and when these two features are enabled, the Telegram on the second device would ask for the Passcode upon launch.

Advisory: Telegram

- For App Developers :
    a. Device Verification at every Launch and when Device change is detected initiate re-registration process.

Facebook and Facebook Messenger are dependent on each other and the access credentials are shared. When Facebook or Messenger or both are restored using MI Mover, both the devices allow the user to access these apps without the need for access credentials and can simultaneously chat or post messages. Theoretically, this cannot be termed a flaw, since Facebook allows installation and access from multiple devices. However, we find that there is no notification related to access to Facebook from the second device. Normally, when a User installs and logs on to Facebook from the second device a notification is sent, however, in this case, it is not so.

Moreover, the two sessions from these two devices are not recognized and only one session out of the two is shown as Active, although both of them are active. Secondly, the session list show in Facebook is more of an Audit Log, does not convey the actual number of connected devices. Since Facebook allows termination of a session, it has a detrimental effect out of the two devices anyone out of the two devices would be allowed access without a password.

Advisory: Facebook / Messenger

- For App Developers :
    a. Device Verification at every Launch and when Device change is detected initiate re-registration process.
    b. Identify and enumerate the devices correctly.

| App | Registration/Launch Access restrictions | Credential State | Notification | Session Termination | Severity Impact |
|---|---|---|---|---|---|
| **WhatsApp** | Launched with Full Privileges | Cached | No notification about second session | Not Available | High |
| **Telegram** | Launched with Full Privileges | Cached | No notification about second session | Available. Second Device not identified. Termination results in Re-Registration | Medium |
| **Facebook** | Launched with Full Privileges | Cached | No notification about second session | Available. Second Device not identified. Session List is not unique (Device), have to terminate all the visible sessions. Termination results in logout from both, but any one device can login without being asked for credentials. | Medium |
| **Facebook Messenger** | Launched with Full Privileges | Cached | No notification about second session | Available. Second Device not identified. Session List is not unique (Device), have to terminate all the visible sessions. Termination results in logout from both, but any one device can login without being asked for credentials. | Medium |
| **Twitter** | RegistrationRequired | NA | NA | NA | NO |

SCENARIOS TESTED FOR ACCESS OF APP-SYSTEM STORAGE BY OTHER APPS

| | Yu <-> M1-n | Mi-1 <-> Mi-2 | Yu <-> SG-M1 | SG-M1 <-> SG-M2 |
|---|---|---|---|---|
| **WhatsApp** | No Access | Access Granted – Affected | No Access | No Access |
| **Telegram** | No Access | Access Granted – Affected | No Access | No Access |
| **Facebook** | No Access | Access Granted – Affected | No Access | No Access |
| **Facebook Messenger** | No Access | Access Granted – Affected | No Access | No Access |
| **Twitter** | No Access | No Access | No Access | No Access |

Of all the apps tested under social networking category, Twitter was the only App which has implemented Device Verification.

## CATEGORY: TRANSPORTATION - PRE BACKUP

The only difference between Uber and OLA is that, OLA provides not just wallets but is also moving towards the Utility Payments, Peer-Peer transaction along with providing Ride-Sharing Services. Since wallets are present, peer-to-peer transactions are made available we apply the same fundamentals which we did for Wallets/Banking Apps.

Persistent Login with no TFA gives Uber the Medium Severity, but OLA also provides Peer-Peer transactions with no TFA, which is considered a bigger security issue when compared with that of Uber.

Advisory: Uber

- For App Developers :
  a. Implement TFA while accessing Wallet
- For End-Users :
  a. Implement App Locker.

Advisory: OLA

- For App Developers :
  a. Implement TFA while accessing Wallet and while transferring money.
- For End-Users :
  a. Implement App Locker.

| App | Registration | Login | During Launch | Wallet / Payment | Peer to Peer Transactions | Severity Impact |
|---|---|---|---|---|---|---|
| **Uber** | Mobile + Password | OTP / Password | Persistent Login | TFA not implemented | Not available | Medium |
| **OLA** | Mobile + Password | OTP / Password | Persistent Login | TFA not implemented | TFA Not implemented | High |

## CATEGORY: TRANSPORTATION - POST RESTORE- S2 (BETWEEN TWO XIAOMI DEVICES)

Uber app was launched after being restored to a new device, and it started normally. It did not recognize the new device. Additionally, the history, wallets were accessible without any TFA, which ideally should be considered mandatory.

Advisory:

- For App Developers :
    a. Device Verification at every Launch.
    b. When Device change detected at least ask for Access Credentials or reinitiate the registration process.
    c. Enforce Server-side verification of MPin / Passcode.
    d. Authenticated Session termination.
    e. Login Notification.

OLA app, after restore launched without needing the user to provide any credentials nor is there any form of device verification present at the time of launch. Moreover, since OLA is also providing Peer-to-Peer transactions, Utility Bill Payment along with providing the facility for hailing/sharing rides, it is all the more important for OLA to provide TFA while allowing its users to access the app.

Advisory:

- For App Developers :
    a. Device Verification at every Launch.
    b. When Device change detected at least ask for Access Credentials or reinitiate the registration process.
    c. Enforce Server-side verification of MPin / Passcode.
    d. Authenticated Session termination and Login Notification.

| App | Registration/Launch Access restrictions | Credential State | Device Validation | Online Payment | Availability of Session Termination | Severity Impact |
|---|---|---|---|---|---|---|
| **Uber** | Credentials not asked. Launched with full privilege | Cached | None | Allowed without TFA | No | Medium |
| **OLA** | Credentials not asked. Launched with full privileges. | Cached | None | Allowed without TFA. Peer-to-Peer , Utility Payments etc. allowed without TFA | No | High |

SCENARIOS TESTED FOR ACCESS OF APP-SYSTEM STORAGE BY OTHER APPS

| | Yu <-> M1-n | Mi-1 <-> Mi-2 | Yu <-> SG-M1 | SG-M1 <-> SG-M2 |
|---|---|---|---|---|
| **Uber** | No Access | Access Granted – Affected | No Access | No Access |
| **OLA** | No Access | Access Granted – Affected | No Access | No Access |

What would happen when two different users, initiate the rides from different locations, using these two cloned devices, was a scenario which hasn't been put to test and we believe it would provide interesting insights into the internal functioning of the analytics algorithms used.

## CATEGORY: SHOPPING - PRE BACKUP

With the advent of e-commerce, mode of conducting business, delivery and payment has changed drastically. Retail and Wholesale markets have changed, and due to increase in available bandwidth and network speeds, additional services like VOD, Live streaming have been introduced and along with it new challenges related to Piracy and DRM have emerged. Online retailers have been providing apps with wallets, gift cards, vouchers, offers and much more to their customers and have also been tackling the menace of fraud. Due to the fact that some of the Apps provide gift cards, hence restricting access to this specific section would highly appreciated.

Advisory:

- For App Developers :
  a. Auto-lock or session timeout.
  b. Implement TFA when Cash on Delivery is chosen.
- For End-Users :
  a. Implement App Locker.

| App | Registration | OTP | During Launch | Gift Cards / Credit – Debit Cards | TFA | Auto-Lock | Severity Impact |
|---|---|---|---|---|---|---|---|
| **Amazon** | Email-id , password, mobile no | Mobile OTP | Persistent Login | Yes. Cards Saved | Banking / Wallet TFA | No | Low |
| **Amazon Prime Video** | Email-id , password, mobile no | Mobile OTP | Persistent Login | Yes. Cards Saved | Banking/Wallet TFA | No | Low |
| **Flipkart** | Email-id , password, mobile no | Mobile OTP | Persistent Login | Yes. Cards Saved | Banking / Wallet TFA | No | Low |
| **SnapDeal** | Email-id , password, mobile no | Mobile OTP | Persistent Login | Yes. Cards Saved | Banking/Wallet TFA | No | Low |

## CATEGORY: SHOPPING - POST RESTORE- S2 (BETWEEN TWO XIAOMI DEVICES)

Amazon and Amazon Prime Video, upon getting restored, allow unhindered access to all the areas including the Gift Card section, saved cards etc., which can allows the user of the second device to use the gift cards and the saved cards, while Amazon Prime Video on the second device allows access to all the downloaded content, since, during restore all the downloaded content is also synced, moreover it seems this is not in accordance with their DRM Policy. From the end-user point of view this cannot be termed as a flaw, however would this be acceptable to Amazon?

Flipkart and SnapDeal, too allow access to all the areas including the secure areas related to cards, however banking credentials are required for conducting these transactions, hence the overall impact is low. However, access to buying history, addresses etc. are related to privacy and all the apps provided unrestricted access.

Advisory:

- For App Developers :
  a. Device Verification at every Launch.
  b. When Device change detected at least ask for Access Credentials or reinitiate the registration process.

| App | Registration/Launch Access restrictions | Credential State | Device Validation | Online Payment | Availability of Session Termination | Severity Impact |
|---|---|---|---|---|---|---|
| **Amazon** | Credentials not asked. Launched with full privileges. | Cached | None | Banking TFA, Saved Cards accessed. History Available | No | Medium |
| **Amazon Prime** | Credentials not asked. Launched with full privileges. | Cached, Downloaded Videos Available. | None | NA. | NA | Low |
| **Flipkart** | Credentials not asked. Launched with full privileges. | Cached | None | Banking TFA, Saved Cards accessed. History Available | No | Medium |
| **SnapDeal** | Credentials not asked. Launched with full privileges. | Cached | None | Banking TFA, Saved Cards accessed. History Available | No | Medium |

SCENARIOS TESTED FOR ACCESS OF APP-SYSTEM STORAGE BY OTHER APPS

| | Yu <-> M1-n | Mi-1 <-> Mi-2 | Yu <-> SG-M1 | SG-M1 <-> SG-M2 |
|---|---|---|---|---|
| **Amazon** | No Access | Access Granted – Affected | No Access | No Access |
| **Amazon Prime Video** | No Access | Access Granted – Affected | No Access | No Access |
| **Flipkart** | No Access | Access Granted – Affected | No Access | No Access |
| **SnapDeal** | No Access | Access Granted– Affected | No Access | No Access |

## CATEGORY: SECURE DOCUMENTS

DigiLocker was the only application in this group which was tested and they have there is nothing to complain about. After initiating restore too, this application needed the access credentials. However, it is to be noted that, although DigiLocker provides the users with Cloud Storage, but users may download the document on to their devices and these documents are accessible to all the applications and can be shared with anyone.

| App | Registration | Launch | Severity Impact |
|---|---|---|---|
| **DigiLocker** | Username /Password / Aadhar | Asks for username / password every time | None |

## CONCLUSION AND REMEDIATION

Xiaomi's system apps have unknowingly introduced multiple flaws into the functional working of most of the apps. The functional aspects of Anti-Theft security apps and Android for Work apps are affected by the un-install procedure implemented by Xiaomi. Furthermore, the MI-Mover app which assists in user-data migration also poses significant threats to the installed apps. Although, Xiaomi alone cannot be held responsible; the app developers are also equally responsible for not taking into consideration that there existed a huge possibility of their application's app-system-data getting cloned/copied. This particular use-case existed since the day, devices started getting rooted and app-system-storage was compromised. It's surprising that app developers never realized that the data which they are storing on app-system-storage is vulnerable on rooted phones. Although Xiaomi's MI Mover allows the users to copy all their data, it goes one step ahead and copies from the app-system-storage areas too.

Cloned Xiaomi device affects the functional security controls related to factors governing access control mechanisms i.e. Identification, Authentication and Authorization implemented by the Third Party Apps. The un-installation procedure implemented by Security Apps is adversely affected on Xiaomi Devices. Apps based on the guidelines provided for implementing Android for Works are affected by the improper implementation of un-installation procedure implemented on Xiaomi devices.

There is another line of argument, which states that – "Physical access to the victim's phone is required". All said and done, yes its true physical access to the phone is required but this raises a few more questions.

- What precautions do Xiaomi device users have to take into consideration, while handing over their devices to Service Centre Employees?
- How should Xiaomi users ensure that their device doesn't get stolen?
- *Repudiation is the most worrisome factor.*

Hence, all the App Developers which have access to sensitive and critical end-user information and are paranoid about the security should consider implementing the following so as to overcome the flaw introduced through the usage of MI-Mover and Backup apps relying on rooted devices.

a. Device Verification at every Launch.
b. Auto Lock Sessions and Authenticated Session termination.
c. When Device change is detected,
    a. Request Access Credentials and compare them with the credentials stored on the server.
    b. Initiate Registration process.
d. Audit Trail of Access and Login Notification.
e. Security Apps and Android For Work App developers should specifically test all the functionalities of their apps on Xiaomi devices.

Device owners, administrators should consider following these broad guidelines

1: Not to use MI-Mover to share apps, but should rely on ShareIT or Xender or any other file/app sharing applications.

2: Not enable Smart-Lock, which is related to automatically unlocking your device.

3: Update the Patch which will be made available by Xiaomi as per their release schedule.

4: Validate the features of Security Apps and Android for Work Apps

| | App-System-Storage | App Data after Restore | Root Access Required | Impact |
|---|---|---|---|---|
| **MI-Mover** | Can Access | Yes – available on second Xiaomi device | No | App Developers and Users |
| **Smart Switch** | No | No | NA | No Impact |
| **Xender** | | No | NA | No Impact |
| **ShareIT** | No | No | NA | No Impact |
| **Titanium Backup** | Requires Device to be Rooted | Without Root – No | Yes | After gaining Root Access |
| **Helium** | Requires Device to be Rooted | Without Root – No | Yes | After gaining Root Access |

## COPY APP SYSTEM STORAGE AREA – POST RESTORE (DEVICES HAVEN'T BEEN ROOTED)

| | Yu <-> M1-n | Mi-1 <-> Mi-2 | Yu <-> SG-M1 | SG-M1 <-> SG-M2 |
|---|---|---|---|---|
| **Goibibo** | No Access | Access Granted | No Access | No Access |
| **Yatra** | No Access | Access Granted | No Access | No Access |
| **MakeMyTrip** | No Access | Access Granted | No Access | No Access |
| **Airbnb** | No Access | Access Granted | No Access | No Access |
| **IRCTC** | No Access | Credentials not stored locally | No Access | No Access |
| **PayTM** | No Access | Access Granted | No Access | No Access |
| **JioMoney** | No Access | Credentials not stored locally | No Access | No Access |
| **WhatsApp** | No Access | Access Granted | No Access | No Access |
| **Facebook** | No Access | Access Granted | No Access | No Access |
| **Facebook Messenger** | No Access | Access Granted | No Access | No Access |
| **Telegram** | No Access | Access Granted | No Access | No Access |
| **Twitter** | No Access | Device Verification Enabled | No Access | No Access |
| **Uber** | No Access | Access Granted | No Access | No Access |
| **OLA** | No Access | Access Granted | No Access | No Access |
| **Amazon** | No Access | Access Granted | No Access | No Access |
| **Amazon Prime Video** | No Access | Access Granted | No Access | No Access |
| **Flipkart** | No Access | Access Granted | No Access | No Access |
| **SnapDeal** | No Access | Access Granted | No Access | No Access |
| **DigiLocker** | No Access | Credentials not stored locally | No Access | No Access |

## APPENDIX A - POC

Real-time encryption and the keys which are generated in real-time are always unique for every device and two different devices would always generate two different set of keys. However, when an App starts generating same set of keys for two different physical devices then we can definitely state that the app's method of implementing the encryption is broken and same random number is being generated.

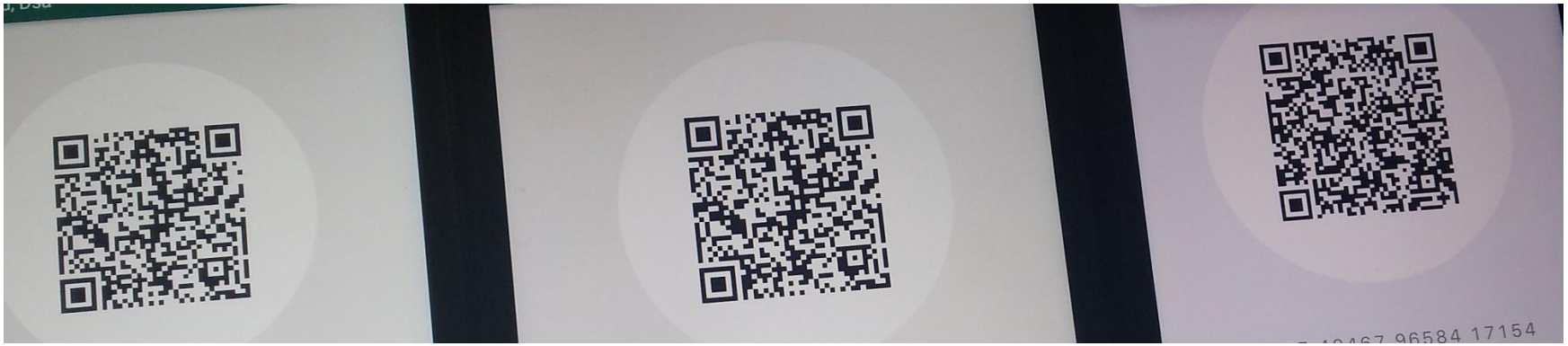
MI-Mover by way of backup and restore has introduced vulnerability in majority of the apps, which otherwise are considered safe. WhatsApp provides us a way to view the encryption keys generated for peer-to-peer communication and the same is made available for verification purposes.

| Device | Key Number | QR Code | Text QR-Code Read |
|---|---|---|---|
| **MI Model 1** | 39597 40467 96584 1715461008 29090 57584 6680765411 44306 99388 00955 | Same | 91390350-91078359 |
| **MI Model 2** | 39597 40467 96584 1715461008 29090 57584 6680765411 44306 99388 00955 | Same | 91390350-91078359 |
| **iPhone** | 39597 40467 96584 1715461008 29090 57584 6680765411 44306 99388 00955 | Different | 91078359-91390350 |

From this it is quite evident that

- There is a communication channel open between iPhone and both of the MI Phones.
- Both the MI Phones have the same encryption keys and their QR code is also the same. This denotes that WhatsApp configured on the MI Phones is for the same Mobile Number.

From the available image use a Barcode Scanner to view and verify the details.



## APPENDIX B – VENDOR RESPONSE

On June 20, 2017 we started contacting all the affected vendors, however except for Facebook; none of the vendors reverted back. There were some vendors who used Third-Party Vulnerability Reporting Services which required the reporter to have sufficient vulnerability report points at that particular platform. Some vendors have put in place their bug reporting mechanism while for other it was by sending out tweets.

The response by Facebook's Security Team confirms with our initial findings and our analysis too.

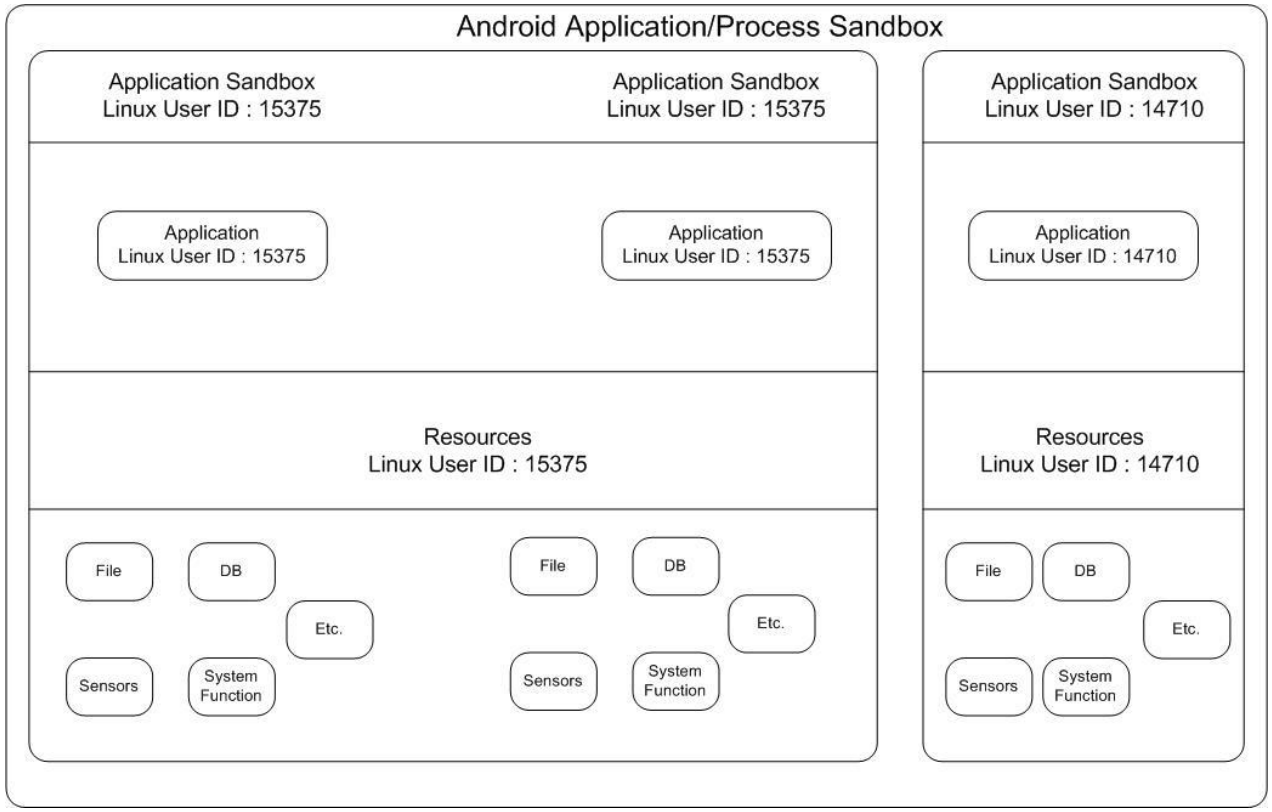
> "As part of exploiting the issue you describe, someone needs to take control of a user's mobile phone and get that phone in an unlocked state. This is a very high barrier to entry and seems unlikely to happen commonly, making this more of a theoretical attack. The protection in this case is to not allow someone to steal and unlock your phone."

As on July 19th and 20th, 2017 this document has been submitted to Xiaomi, most of the app developers and IT Security Specialists for peer review.

| Vendor | Response Summary |
|---|---|
| **Facebook** | Theoretical bug, the end-user has to protect the phone from getting stolen and has to implement pattern/Passcode on the device. |
| **WhatsApp** | They may not implement the suggestions immediately. |
| **PayTM** | Patched. However, they haven't yet reverted back with the acknowledgement. |
| **Goibibo** | Awaiting reply |
| **ICICI** | Patched. They requested to increase the scope of this research to include other banking apps. |
| **SnapDeal/ Freecharge** | Awaiting reply |
| **Amazon** | Awaiting reply |
| **Flipkart** | Awaiting reply |
| **Ola** | Not a bug. |
| **Xiaomi** | They shall be issuing a patch as per the schedule and the date hasn't been mentioned. |

# APPENDIX C - ANDROID SANDBOX MODEL

Let us understand a few basics about Android's Sandbox Model. Android implements what is known as Application Sandbox, wherein Android doesn't allow an application to access the resources of another app? Every app is given a unique user-id (UID) and the android system executes that app as a separate process with that specific UID, effectively isolating that app and its resources from other apps, moreover processes with same UIDs can share resources amongst themselves. Furthermore, when Applications need to use functionality / capabilities viz. accessing Contacts, Camera, GPS etc. before installation begins, the applications have to request for these permissions from the user.




Alternatively, we can infer that when an app tries to access the app-system-storage of another app then Android System protects against this, since the offending app doesn't have the right privileges.

According to Google's Android Team - "Like all security features, the Application Sandbox is not unbreakable. However, to break out of the Application Sandbox in a properly configured device, one must compromise the security of the Linux kernel."

From this it is quite evident that other than the Android System Apps, Third party end-user apps cannot interact with the App-System-Storage. Furthermore, when the device is rooted, for any app with root privileges it would be now possible to bypass the boundaries enforced upon by the Android System.

## APPENDIX D - REFERENCES

1. **Android Security** : https://static.googleusercontent.com/media/enterprise.google.com/en//android/static/files/android-for-work-security-white-paper.pdf
2. **Android Kernel Security** : https://source.android.com/security/overview/kernel-security
3. **Android Security Mechanism** : http://blog.h1994st.com/android-security-mechanisms/
4. **Information Security** : https://en.wikipedia.org/wiki/Information_security
5. **CIA Triad** : http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
6. **Access Control** : https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems
7. **Market Share** : https://www.androidheadlines.com/2017/05/counterpoint-samsung-no-1-india-followed-xiaomi.html
8. **Market Share** :http://indianexpress.com/article/technology/tech-news-technology/idc-q4-2016-xiaomi-lenovo-chinese-players-dominate-indian-players-out-4522342/
9. **Butterfly Effect** : https://en.wikipedia.org/wiki/Butterfly_effect