Investigation Of Contemporary Attacks In Android Apps

M.Kireet, Pavithra rachala, Dr.Meda Sreenivasa Rao, Rukmini Sreerangam

Abstract: This paper investigates the recent attacks in android Smartphone's. The popularity of using the android smartphones has increased immensely all over the world which made the malware writers to target android as major platform to introduce different type of attacks and extract user sensitive information. This paper gives the brief study and solutions on the recent six malware attacks namely Man-in-the-disk attack, Attacks using Fake apps, Attacks through privacy violation, Attacks due to Pre-installed apps, Collaborating apps, Attacks through outdated apps in android smartphones. All the attacks mentioned in this study does not have proper solutions which are leading to extraction of sensitive user information. Most of the attacks mentioned use the loopholes provided by developers in developing the apps. Finally, this paper provides the analysis of latest attacks with the best possible solutions to enhance the android app detection.

Index Terms: Man-in-the-disk attack, Attacks using Fake apps, attacks through apps, collaborating apps, malware writers, pre-installed apps, attacks through privacy violation

1 INTRODUCTION

The usage of android Smartphones in the past five years has been drastically increased. As a result majority of apps are being developed in android environment due to its open-sourced nature. The basic traditional corporate liable model BYOD(Bring Your own Device) followed by most of the enterprises, giving provisions for users to run third party apps are the two major reasons which are making the android smartphones vulnerable to different type of attacks[1]. There are different type of attacks where the Smartphone can be attacks from the previous studies which include spyware attacks[2], the Phishing attacks[3], Worm-Based-attacks[4], Botnets[5], Financial Malware attacks Permission leakage attacks[7]. Most of the attacks mentioned have detection methods. But day-by-day attackers are finding out the news ways to bypass the present android security provisions. In this paper we worked to identify the new type of attacks which do not have a proper security provisions, we have taken the data from the Professional Research reports [7], hacker blogs and professional news forums to identify the recent attacks on the android apps. Finally, we conclude about the type of attack, its vulnerability and effected smartphones till date. These type of attacks have been mentioned as Vulnerabilities in Standard website

The following figure shows the overview of transactions which are done through mobile apps.

Fig 1 *.Overview of the transactions done through mobile apps*

2 RECENT ATTACKS IN ANDROID SMARTPHONES

Security analysts, Research reports[7], professional hacker forums[8] have reported these attacks which does not have a proper solution as a result many android smartphones were vulnerable to attacks. The attacks reported are MITD(Man-in-the disk attack, attacks using Fake apps, attacks through apps, attacks through privacy violation, collaborating apps, attacks through outdated apps in android smartphones.

2.1 MITD(Man-in-the-disk attack)

Security analysts from checkpoint [9][10] recently found that android smartphones are vulnerable to Man-in-the-disk attack Man-in-the disk attacks are also called as Man-in-the device attacks. Many of the apps which were developed and distributed by popular developers like Google are susceptible to MITD attacks. These MITD attacks are similar to that of man-in-the middle attacks where both type of attacks initially intercept and later modify the data by the attacker intended purposes. MITD attacks can have a potential to damage the android smartphones, and they also damage the reputation of the developers as these type of attacks are done because of some of the careless or laziness of developers points. MITD uses the shared workspace of External storage to attack where most of the apps developed by the developer use the External storage in unsafe way. To understand this type of attack in detail first android storage function or usage needs to be explained. Android uses two types of storage for storing the

- *Author name is M.Kireet ,Currentlly working as Assistant Professor in JNTUH college of Engineering Hyderabad, kireet04@gmail.com*
- *Co-Author name is Pavithra.rachala ,Currently working as Assistant Professor in CMRTC ,Hyderabad pavithra.rachala@gmail.com*
- *Co-Author name is Dr.Meda Sreenivasa Rao retired Professor,JNTUSIT, Hyderabad ,srmeda@gmail.com*
- *Co-Author name is Rukmini Sreerangam ,Currently working as Assistant Professor in CMRTC, Hyderabad rukumini.sreerangam@gmail.com*

data 1) Internal Storage 2) External Storage. Internal storage of Android is given in a private way to all the apps which cannot be accessed by the other apps. Internal storage can be called as sandbox environment which means the apps in internal storage are isolated and protected from other apps. External storage of Android is shared by all the applications External storage might be a removable disk or memory or it might be a partition on internal memory also. the media files, photos, downloads etc are stored in external storage. Almost every app after installation asks for the permission to access external storage files. As External storage is not sandbox environment all the apps can access, share files on external storage. As per the reports from the researchers most of the apps due to storage related issues are stored in external storage Even the apps stored in internal storage use the external storage by the permission allowance. Malicious attackers are developing the apps which sits on the external storage and extract all the information in external storage. The Scenario of MITD attack Most of the android applications requires large space so the users choose the external storage for storing the larger apps. Considering the game app for demonstrating this attack, the steps are as follows

Step 1 : Attacker installs a similar application to the which has access to all the files in victims smartphone.

Step 2: Assuming Victim is downloading the app from . downloading the game the victim will launch the game which begin downloading the main resources from the web server. Assuming the victim downloaded and stored the game in the external storage.

Step 3: Attacker uses the installed seemingly application application to change or meddle the data of app which is in external storage. Attacker replaces the URL location of the application from where the application request its main resources. In this way the code is tampered.

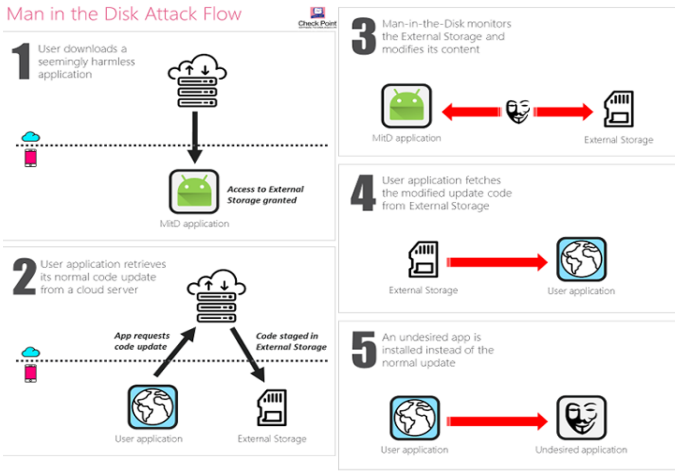


Fig 2. *Overview of MITD attacks*

Step 4: After this successful replacement of code the victim instead of downloading the actual main resources downloads the malicious app injected by the attacker.

Step 5: Finally as the actual app is not downloaded victim may not able to run the app which causes denial of service. In this way Man-in-the-disk or Man-in-the-device interfere and change the contents or data in External storage which leads to MITD attacks. Solutions to stop MITD attacks

1. One of the first solutions to stop MITD attacks is the android app developer's needs to follow guidelines provided by the android in the usage of External storage.
2. Android provides the application guidelines where most of the developers try fail the usage of external storage with many apps.
3. According to the guideline given by the android when external storage is used by the applications following guidelines need to be followed.
4. Perform input validation when handling data from external storage.
5. Do not store executable or class files on External Storage. External Storage files should be signed and verified prior to dynamic loading.
6. Even the apps developed by the Google developers are not following the guidelines when external storage is used in apps.

2.2 ATTACKS USING FAKE APPS

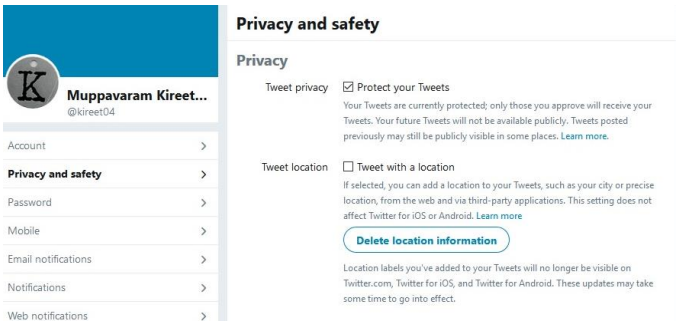
The vast expansion of Smartphone usage has drastically increased the development of different type of apps. The common man is much dependent on apps to perform his daily activities easily. This is giving a platform for the malware writers to initiate malware apps by making a fake app of popularly used apps. The users to remember that just because of the apps are installed from Google do not give the guarantee of the app whether the app is genuine or safer app. Many apps which are developed by Google developers have also turned as malicious apps by releasing sensitive information as per different standard report[11][12]. What is the intent of Fake apps : Fake apps are developed by malware writers and make them popular by fake reviews/recommendations. The users install the fake apps and when the user attempts to use the appthe app asks the user to update the app for smoother functionality and to get furthermore utilities. The user unknowingly updates the app which might apply a phishing technique and extract the user sensitive details. Google has recently removed 29 camera related apps from the which are Fake apps. These 29 apps initially are downloaded from and after installing when specific camera or beautify function is initiated, the app instead of displaying the final result asks the user to update the app in nine other different languages leading to phishing attack. The following are the list of fake apps removed recently from by Google[8]

App name	*App Name*
Procamera beauty	*Cartoon art photo filter*
Cartoon art photo	*Art Filter Photo Editor*
Emoji camera	*Picture*
Artistic effect Filter	*Art Effect*
Art Editor	*Photo art effect*
Beauty Camera	*Cartton Photo Filter*
Selfie Camera Pro	*Art Effect*
Horizon-beauty camera	*Photo Editor*
Super Camera	*Wallpapers HD*
Art Effect for photo	*Magic Art Filter Photo Editor*
Awesome Cartoon art	*Fill Art Photo Editor*
Art Effect for Photo	*ArtFlip Photo Editor*
Art Filter Photo	*ArtFlip Photo Editing*
Art Filter Photo Effects	*Art Filter*
Cartoon Effect	*Cartoon art photo*
	Prizma Photo Effect

The above table shows the list of fake camera apps which ask for an update when the app is run by the user after installation
Solutions and Challenges identify Fake apps:
The following are the basic solutions to identify Fake apps
Most of the Fake apps are downloaded from websites or links which have been forwarded through SMS or social networking messages in user mobiles. The best possible solution is any app when downloaded by the users should be downloaded from Play store. The users before installation should look at the reviews of the app. If any users who have previously downloaded the apps might review the performance of the app based on the ratings the user if finds any negative solutions have to stop installing the app. The above two solutions are the most common solutions which could not identify the most of the latest fake apps. There is biggest challenge in this area for the researchers to identify whether the app is fake app or genuine app.

2.3 ATTACKS DONE THROUGH PRIVACY VIOLATION/ MISCONFIGURATION:

There are some apps which have misconfigurations in their settings and there are also some more apps which were developed by violating the privacy principles. Most of the attackers concentrate towards the faults in the app which might occur due to carelessness of developers or some times unknowingly violate the privacy principles. such kind of loopholes exist in apps attackers extract the sensitive information from those loopholes Following example shows how the attacker can extract the sensitive information when privacy principles are violatedRecently a report [15] that twitter bug left android users private tweets exposed for four years



The above figure shows that “protect your tweets “ in tweet privacy in settings when the users are signup in twitter by default all the tweets are public If the tweet privacy is chosen by enabling the “protect your tweets” option all the tweets will be made private and the tweets will be visible to the friends who follow your account with users permission. Most recently twitter has posted that a privacy bug has caused the twitter app to disable “protect your tweets” by which all the tweets of many users are publicly available though they have chosen their privacy in settings which made many hackers to extract the user sensitive information easily. Apparently twitter has fixed the bug by updating the app.
Solutions and Challenges in identifying the attacks done through misconfiguration/Privacy violation:

1. The best solution is identifying these type of attacks at present is to observe the performance of the mobile when app is running if the user's smartphone is not giving the desired performance then all the settings need to be checked
2. Most of the users will not update the apps in regular basis which had a greater impact when the developers resolve the app issues, so the app resolves some problems related to misconfigurations or any privacy violation The above example clearly explains how once the twitter privacy settings has , once it is identified twitter updated the app to resolve the issue
3. The biggest challenge in identifying this attack is identifying the privacy-violation; most the apps unknowingly developed by the developers are causing big damage to the app in terms of financial transactions. In the initial usage of financial apps apps like , amazon has faced this problem later these problems were identified A Strong security mechanism which identifies the privacy bug's and misconfiguration is still a challenging task.
4.

2.4. ATTACKS DUE TO PRE-INSTALLED APPS

Any app that is installed on system partition appis called apps. Most of today’s Smartphones are released into the market by installing some apps. By the time user starts using his new android Smartphone almost above 10 apps related to Google apps like Google chrome, Google Play, Google translate etc are in new Smartphone. The vulnerabilities in apps are giving provision for the attackers to extract the user sensitive information. All of the apps which execute can obtain the permissions with an android: ProtectionLevel of signature or system. System or Signature Protection permissions are not obtained by the third-party apps. Some of the vulnerabilities in apps will dump Pesonal Identifiable Information into the External storage. Third party appsor any type of apps which are installed if they have READ_EXTERNAL_STORAGE permission then the sensitive information provided by apps can be accessed by any app.
Following are the list of vulnerabilities reported [16] in different smartphones.

Sno	*Android Device*	*Vulnerability*
1.	*Asus ZenFone V Live / Asus ZenFone Max 3*	*Arbitrary command execution as system user*
2.	*Asus ZenFone V Live / Asus ZenFone Max 3*	*Take screenshot*
3.	*Asus ZenFone 3 Max*	*Dump bugreport and Wi-Fi passwords to external storage*
4.	*Asus ZenFone 3 Max*	*Arbitrary app installation*
5.	*Essential Phone*	*Programmatic factory reset*
6.	*ZTE Blade Spark / ZTE Blade Vantage /*	*Dump modem and logcat logs to external storage*
7.	*ZTE Zmax Champ / ZTE Zmax Pro*	*Dump modem and logcat logs to*

		external storage
8.	LG G6 / LG Q6 / LG X Power / LG Phoenix 2	Dump logcat log to attacking app's private directory
9.	LG G6 / LG Q6 / LG X Power / LG Phoenix 2	Lock the user out of their device (requiring a factory reset to recover in the most cases)
10.	Coolpad Defiant / Tmobile Revvl Plus	Programmatic factory reset
11.	Coolpad Canvas	Dump logcat log, kernel log, and tcpdump capture to external storage
12.	Coolpad Canvas	Change system properties as the com.android.phone user
13.	ZTE Zmax Champ	Programmatic factory reset
14.	Orbic Wonder	Programmatic factory reset
15.	Orbic Wonder	Writes content of text messages and phone numbers for placed/received calls
16.	Alcatel A30	Take screenshot
17.	Nokia 6 TA-1025	Take screenshot
18.	Sony Xperia L1	Take screenshot
19.	Leagoo Z5C	Programmatic factory reset
20.	MXQ 4.4.2 TV Box	Programmatic factory reset
21.	SKY Elite 6.0L+	Arbitrary command execution as system user
22	Oppo F5	Record audio (requires vulnerability above to transfer file to attacking app's private directory)
23.	Leagoo P1	Take screenshot
24.	Leagoo P1	Programmatic factory reset
25.	Vivo V7	Video record the screen and write it to the attacking app's private directory
26.	Vivo V7	Dump the logcat and kernel logs to SD card
27.	Vivo V7	Change system properties as the com.android.phone user allowing the coordinates of touch and gesture data to the logcat log

As per different standard reports below are some of the commands which uses system user command.

Sno	Command	Functionality in terms of Vulnerability
1.	system/bin/screenrecord--time-limit60/sdcard/sixtyseconds.mp4	This command records the user's screen for 60 seconds
2	/system/bin/settings put secute enabled_notification_listenerscom.mmy.app/NotSomeNotificationListenerService	This command sets your app as a notification listener
3.	/system/bin/settings put secure selected_spell_checker com.my.app/.NotSomeSpellCheckingService	This commandSet your app as a spell checker providing partial keylogger functionality
4.	system/bin/settings put secure enabled_input_methods <ones that were already there>:com.my.app/.NotSomeKeyboardService /system/bin/settings put secure default_input_method com.my.app/.NotSomeKeyboardService	This command sSet your app as the default IME (e.g., keyboard) for keylogger functionality
5.	system/bin/logcat -d -f /sdcard/notthelogdump.txt /system/bin/logcat -f /sdcard/notthelog.txt	This command Obtain the logcat log
6.	system/bin/input tap 560 1130 /system/bin/input swipe 540 600 540 100 200 /system/bin/input keyevent 3 66 67 66 /system/bin/input text scuba	This command Inject touch, gestures, key events, and text
7.	am start -a android.intent.action.CALL_PRIVILEGED -d tel:800-555-5555	This commandCall a phone number (can be used to call emergency numbers)
8.	android.intent.action.MASTER_CLEAR	This command Factory reset the device
9.	content query --uri content://sms	This command get's all of the user's text messages
10.	content query --uri content://call_log/calls	This command get's all of the

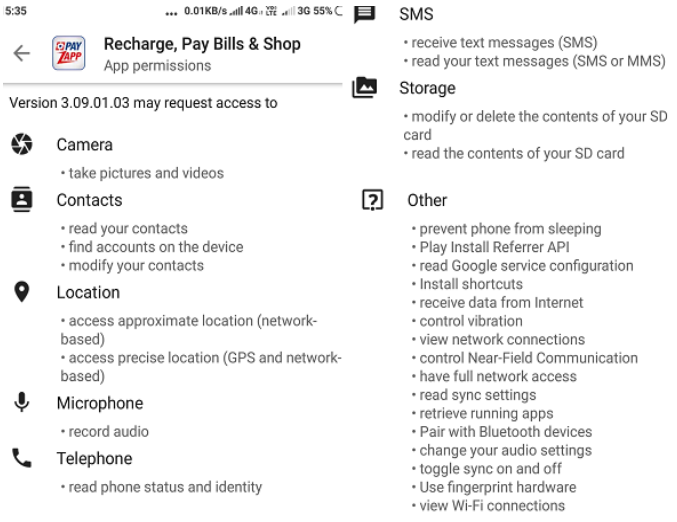
		user's call log
11.	*content query --uri content://contacts/people*	*Get all of the user's contacts*
12.	*setprop persist.sys.diag.mdlog 1*	*This command set certain system properties*
13.	*settings put secure install_non_market_apps 1*	*This command change arbitrary settings*
14.	*pm disable com.some.undesirable.app*	*This command disabled third-party apps*

Solutions and challenges to identify the attacks done through apps

- There is no particular mechanism available to check the apps this is the biggest challenge in the area of mobile security.
- There are few detection models in terms of Permission based detection which could not solve the complete identification of attacks through apps.

2.5. COLLABORATING APPS

Most of the apps in the category of Finance, shopping are collaborating with Google apps. Almost of 90% of smartphone are using any of the Finance or Shopping apps. At the time of registration of this Finance, shopping apps the users are given provision to use the apps by signing up as new user or by signing up with Google id. The provision of using the app by Google ID is making the different apps like Financial, shopping apps to collaborate and share the confidential information of the user which is against to the privacy rules.
considering the app as an example. The following figure shows the permissions requested by the app.



The uses the permissions specified in the app requested permissions. The same app needs the user to login by registration privately with new user id or even user can use the google id to login the same app. When the user uses existing Google ID for the login for app permissions will collaborate with permissions as a result it leads to provide the app with more permissions than the required permissions which leads to privacy issues.

2.6. ATTACKS DUE TO OUTDATED APPS

Most of the apps initially released with some bugs into the app store. The developers sometimes unknowingly and sometimes due to their carelessness release the apps with bugs. The bugs were identified with bugs the developers release the patches in the form of updates to the app. Most of the smartphone users for saving the mobile data close their automatic updates and such type of users have to manually update their apps. In the process of manual of such kind of apps users use their older versions till the performance of app seems to be slow. This usage of outdated apps giving a provision for the attackers to introduce DOS attacks through apps which makes the app run slower and sometimes may stop the app service. McAfee standard reports[18] in 2016 has suggested that constant needed for all the apps to prevent the apps from the following Stealing the user sensitive information from the mobiles, Protection from reading your personal or work emails, other file, to stop sending fake text messages on your behalf, loading viruses into your phone without your knowledge etc.

3. CONCLUSION

This paper summarizes the most common recent six type of attacks on android smartphones based on the reports given by standard vulnerability report CVE(Common Vulnerability reports DEFCON report on in US Election equipment databases, professional hacker forums. These types of attacks like MITD attacks, Fake apps, attacks through apps are the challenges in the present scenario in the android smartphones' environment. The present security provisions and various app detection models by the researchers have not addressed the risks posed by these attacks. We addressed the common solutions for these recent attacks, most of the addressed solutions are commonality solutions and there is a future scope for the researchers to address all types of attacks and check the app is safer or not before it is installed by the user into his smartphone, thus the need for the app security services will be solved.

REFERENCES

[1] D. Sbîrlea, M.G. Burke, Salvatore Guarneri " Automatic detection of inter–application permission leaks in android applications, technical report tr13-02,dept of cse, Rice university, Research Report, IBM Journal of Research and Development, Volume: 57 , Issue: 6 ,Nov.-Dec. 2013, DOI: 10.1147/JRD.2013.2284403

[2] Fan Wu, Hira Narang, Dwayne Clarke "An Overview of Mobile Malware and Solutions" Journal of Computer and Communications, 2014, 2, 8- 17Published Online October 2014 in SciRes. doi.org/10.4236/jcc.2014.212 ,

[3] S. Peng, "A Survey on Malware Containment Models in Smartphones", Applied Mechanics and Materials, vol. 263-266, pp. 3005-3011, 2013

[4] Jamaluddin, N. Zotou, P. Coulton, "Mobile phone vulnerabilities: a new generation of malware", Proc. IEEE International Symposium on Consumer Electronics, pp. 199-202, 2004

[5] Muppavaram K., Sreenivasa Rao M., Rekanar K., Sarath Babu R. (2018) How Safe Is Your Mobile App? Mobile App Attacks and Defense. In: Bhateja V., Tavares J., Rani B., Prasad V., Raju K. (eds) Proceedings of the Second International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and

Computing, vol 712. Springer, Singapore Print ISBN 978-981-10-8227-6 DOI: https://doi.org/10.1007/978-981-10-8228-3_19 2018
[6] M. Kireet, Dr. Meda Sreenivasa Rao. "Investigation of Collusion Attack Detection in Android Smartphones." International Journal of Computer Science and Information Security, (IJCSIS) Vol. 14, No. 6, June 2016
[7] Portal, Statistics. Share of Android OS of global smartphone shipments from 1st quarter 2011 to 2nd quarter 2018" https://www.statista.com/statistics/236027/global-smartphone-os-market-share-of-android/ (2018)
[8] Mohit kumar, Swathi Khandelwal A Research report on
[9] Cyber attacks in Professional Hacker forums https://thehackernews.com/
[10] Slava Makkaveev "Man-in-the-Disk: Android Apps Exposed via External Storage" https://research.checkpoint.com/androids-man-in-the-disk/ Aug 2018
[11] Research Report by Guardian Project https://guardianproject.info/2018/08/17/iocipher-is-the-antidote-to-man-in-the-disk-attack/
[12] Kaspersky Secutiy Bulletin:" Kaspersky Report on MITD attacks" 2018 https: https://www.kaspersky.com/blog/man-in-the-disk/23622/
[13] B. Andow, A. Nadkarni, B. Bassett, W. Enck, and T. Xie, "A study ofgrayware on Google Play,"2016 IEEE Security and Privacy Workshops(SPW), pp. 224–233, 2016
[14] S. Chen, M. Xue, L. Fan, S. Hao, L. Xu, H. Zhu, and B. Li, "Automatedpoisoning attacks and defenses in malware detection systems: Anadversarial machine learning approach,"computers & security, vol. 73,pp. 326–344, 2018.
[15] S. Chen, M. Xue, and L. Xu, "Towards adversarial detection of mobilemalware: poster," inProceedings of the 22nd Annual InternationalConference on Mobile Computing and Networking.ACM, 2016, pp.415–416
[16] Twitter bug reported in Twitter support : https://twitter.com/TwitterSupport
[17] Reports in CVE Common Vulnerability exposure :https://cve.mitre.org/
[18] [Defcon26: Kryptowire Vulnerable Out of the Box:An Evaluation of Android Carrier Devices "https://media.defcon.org/DEF CON 26
[19] Macafee Reports "Threats prediction : ww.mcafee.com/enterprise/en-us/assets/reports/rp-threats-predictions-2016.pdf "
[20] Kireet .M,Dr.Meda Sreenivasa Rao "A Survey on Malware attacks on smartphones (IJCSIT) " ISSN : 09759646 Volume 6 issue 3 2015
[21] Matt Blaze,Jake Braun "Defcon :Report on Cyber vulnerabilities in US Equipment Document" Worlds second largest Hacker conference 2018