Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2014 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2014

CROSS-SECTIONAL EXAMINATION ON ANDROID SECURITY

Daniel W.K. Tse
Department of Information Systems, City University of Hong Kong, Hong Kong, iswktse@cityu.edu.hk

X .X. Jin
Department of Information Systems, City University of Hong Kong, Hong Kong, xiaoxijin2-c@my.cityu.edu.hk

Y. N. Pan
Department of Information Systems, City University of Hong Kong, Hong Kong, peterpan4-c@my.cityu.edu.hk

Y. Q. Hu
Department of Information Systems, City University of Hong Kong, Hong Kong, yongqiahu3-c@my.cityu.edu.hk

F. Lin
Department of Information Systems, City University of Hong Kong, Hong Kong, fanlin3-c@my.cityu.edu.hk

See next page for additional authors

Recommended Citation

Tse, Daniel W.K.; Jin, X .X.; Pan, Y. N.; Hu, Y. Q.; Lin, F.; and Liu, S. Y., "CROSS-SECTIONAL EXAMINATION ON ANDROID SECURITY" (2014). *PACIS 2014 Proceedings*. 274.
http://aisel.aisnet.org/pacis2014/274

Authors
Daniel W.K. Tse, X .X. Jin, Y. N. Pan, Y. Q. Hu, F. Lin, and S. Y. Liu

CROSS-SECTIONAL EXAMINATION ON ANDROID SECURITY

Daniel W.K. Tse, Department of Information Systems, City University of Hong Kong, Hong Kong, iswktse@cityu.edu.hk

X.X. Jin, Department of Information Systems, City University of Hong Kong, Hong Kong, xiaoxijin2-c@my.cityu.edu.hk

Y.N. Pan, Department of Information Systems, City University of Hong Kong, Hong Kong, peterpan4-c@my.cityu.edu.hk

Y.Q. Hu, Department of Information Systems, City University of Hong Kong, Hong Kong, yongqiahu3-c@my.cityu.edu.hk

F. Lin, Department of Information Systems, City University of Hong Kong, Hong Kong, fanlin3-c@my.cityu.edu.hk

S.Y. Liu, Department of Information Systems, City University of Hong Kong, Hong Kong, shuyiliu6-c@my.cityu.edu.hk

Abstract

Nowadays, mobile terminal has become an indispensable element in people's daily life as the advent of post-PC era, the security issue of these mobile platforms plays a pivotal role in this information technology era. As Android accounts for approximately 80% in the third quarter of 2013, the importance of its potential security risks cannot be neglected. This research started from the critical analysis of the nature of threats from the perspectives of Google and mobile carrier, third-party security applications and user behavior. From these analysis results, a cross-sectional examination was used to derive several practical suggestions for the sake of solving the problems existing currently in the Android phones.

Keywords: Android security, Google, mobile carrier, third-party security applications, user behavior

1 INTRODUCTION

Android is developed by Android, Inc. initially and bought by Google in 2005. It is an operating system (OS) used by mobile devices like smartphones and tablets. According to Framingham (2013) from IDC (International Data Corporation), Android accounted for 81.0% of all smartphone shipments during the third quarter of 2013. It is manifest that the importance of the research on Android security is significant at present. Based on the related works done by previous researchers, this research examined the threats from three perspectives through both quantitative and qualitative methodologies. Specifically, these three perspectives consist of Google, third-party security applications and user behavior, respectively. Google is the owner of Android and it has the official application market, while third-party security applications mean that these applications are developed by third-party market developers, like 360 Security Center. The results of qualitative assessment of both Google & Mobile carrier and third-party security applications illustrate that users behaviors is also the key factor of Android security followed by a quantitative survey developed for the sake of figuring out certain dangerous user behaviors.

2 LITERATURE REVIEW

There are several researches done on the security of Android. Barreba & Oorschot (2011) conducted a research called Secure Software Installation on Smartphones in 2011, and they proposed a comparison between Apple's iOS, Android, BlackBerry, and Symbian installation of third-party apps which had significant implications for mobile devices security. Bing (2012) introduced a comprehensive analysis of the security architecture and potential risks regarding to Android platform in his article Analysis and Research of System Security Based on Android, Han believed that the open-source software and programmable framework characteristic of Android is a double-edged sword which accounts for a large share in the reasons of Android's vulnerability. Bing (2012) proposed that measures should be conducted for preventing intrusions not only on the Linux kernel layer but also on the application layer. Pieterse & Olivier (2012) published a journal article called Android Botnets on the Rise: Trends and Characteristics. They proposed a novel concept called botnet which described that certain type of malware which not only attacked the mobile system but also stole users' personal information in the meantime. Berger, et al (2011) have conducted a case study which is based on an assessment performed by an Android expert with Bauhaus tool-suite for the sake of figuring out the security problems on the platform of Android.

Jeter & Mishra (2013) proposed a research on the Android device users' security risk exposure based on a quantitative experiment. They found that there were several user behaviors which led to the exposure for attackers. Avancini & Ceccato (2013) conducted a technical test of the communication among three Android applications and the results showed that the mismatches between intended behavior declared by an application and the observed functionalities in this application's code did exist. This was a weakness that Android have to deal with.

3 RESEARCH METHODOLOGY

This research has adopted both quantitative and qualitative methods. We have used qualitative approach in the analysis of manufacturer and third-party application market, for which we have investigated a large amount of literatures. Online questionnaire has been used in the assessment of user behaviors.

3.1 Qualitative Methodology

During the analysis from Google and Mobile carrier's perspective, the author has used qualitative approach to analyze comprehensively the existing threats based on related literature. An experiment has been conducted for the sake of assessing the effectiveness of third-party security applications. The following table describes specifically about this experiment.

Experiment Name	An experiment on the effectiveness of Android security applications
Experiment Objectives	1. To test whether Android security applications can effectively detect and

	control over privileged malicious applications’ unauthorized access to user’s private information. 2. To test whether the performances among different Android security application vary from each other significantly. 3. To find areas to improve and make suggestions to security applications developers.
Experiment Background	Due to the open source of Android and the loose control of Android application market, there have been more and more malicious Android applications occur in the market that severely threaten Android mobile security and user privacy. Miler (2011) criticizes the Android Market for its loose control of reviewing apps and allowing ease of entry to malware developers. With the Android security crisis worsens over time, many software companies have made effort to tackle the security crisis. As a consequence, many generations of Android security applications emerge and the security functions become more and more sophisticated and powerful with the technology advancement. Android users’ awareness of the mobile security and the perception on Android security applications vary quite significantly. Some users frequently utilize security application’s sophisticated functions, others occasionally run some elementary security functions, while quite a number of users seldom install any security applications. There are various kinds of Android security applications available in the market, and different users install different security applications on mobile phones, do security applications effectively protect the mobile security and user privacy? The effectiveness of the security applications has become an important area to investigate for researchers and common users.
Experiment Principles and Theories	1. Android malicious applications can stealthily access to and exploit users’ private data or information such as contact numbers, contact records, location, photos, 2. Effective Android security applications can detect and monitor malicious applications that stealthily access to and exploit users’ private data or information, when the malware is being installed or run. 3. The malware in the experiment is already known to be over privilege escalated that it can stealthily access to and exploit users’ private information.
Experiment Assumptions	1. The mobile phone used for experiment doesn’t affect the experiment results. 2. We assume that the design of having two malicious applications as the tested applications eliminates the effects of malicious application itself.
Experiment Subjects	• Experiment platform: Android 2.3.6 on SUMSUNG GT-I9100 • Android security applications: LBE, 360 Mobile Safe, Tencent Mobile Security Master, Lookout Mobile Security, AVG Mobile Security • Malicious applications: 3D Magic Wallpaper, Truth or Dare • 3D Magic Wallpaper: A malicious Android app that stealthily accesses to users’ location information and releases malicious ads exploiting user private information. • Truth or Dare: A malicious Android app that stealthily obtains user privacy and introduces a lot of ads acting maliciously to the mobile phone, which threats the security and privacy seriously.
Experiment Steps	1. Install the LBE Security on the mobile phone, activate its defending mode. 2. Download the “3D Magic Wallpaper” and install it on the mobile phone. 3. Observe whether the security application can detect “Gallery Lock” to be malicious application and warn user of uninstallation of the “3D Magic Wallpaper”. 4. Run LBE scanning to see whether it can detect “3D Magic Wallpaper” to be malicious. 5. Run “3D Magic Wallpaper” to see whether LBE security detects and warns the user. 6. After the experiment on 360 Mobile Safe is done, uninstall “3D Magic

	Wallpaper” and LBE Security and reboot the mobile phone. 7. Repeat the same steps for other Android security applications. 8. Install the LBE Security on the mobile phone, activate its defending mode. 9. Download the “Truth or Dare” and install it on the mobile phone. 10. Observe whether the security application can detect “Gallery Lock” is a malicious application and warn user of uninstallation of the “Truth or Dare”. 11. Run LBE scanning to see whether it can detect “Truth or Dare” to be malicious. 12. Run “Truth or Dare” to see whether LBE security detects and warns the user. 13. After the experiment on 360 Mobile Safe is done, uninstall “Truth or Dare” and LBE Security and reboot the mobile phone. 14. Repeat the same steps for other Android security applications.
Experiment Observations	We test 5 security applications to detect the 2 malware to see whether they can detect the 2 malicious actions: over privileged access to user location information and malicious ads. So there are totally 5*2*2=20 observations for the experiment, and the observation is to see whether the security application can successfully detect the over privileged action. If yes, the observation result is “Y”; if no, the observation result is “N”.

Table 1. The assessment design of the third-party security application.

3.2 Quantitative Methodology

In order to know the users’ behavior which would endanger the security of android smartphone and find out the possible reason why this behavior exists, we chose to conduct a survey using questionnaire.

According to Shan (2010), there are approximately 755 million cell phone subscribers in China and the age group of 25-34 and 35-44 accounted for the largest percentage of users. Also, according to Avancini & Ceccato (2013), the most active users of android system is aged 20-34 and 35-44, therefore we set our target candidates in this range. In order to achieve that, we chose to make a questionnaire online, generating a URL. After that, we sent the URL to social circles using the social networking website and applications. To make our survey cover more candidates, we also added information at the URL to request people to share the URL among their social circles. As a result, most of our candidates are in the range of 20-44.

Considering there are many factors toward a users’ behavior and the method to measure the risk about security, we decided to use scoring, opening and ranking questions. By doing that, we can quantify the risk of each users’ behavior; finding out which one will cause the most severe threats to android smartphone. More specifically, we allocated a level ranging from 1 to 4 or 1 to 6 to each score and rank which will not be shown on the questionnaire. For some questions, we also required candidates to add reasons why they chose these answers so that we can find out the cause of users’ behavior.

Just as Breitinger & Nickel (2010) mentioned that, as the number of mobile phones, their functionalities and application scenarios increases, it is very important to find out a pattern among them. We planned to do the survey from two aspects. The first is about the users’ general awareness of security while the second is about the specific behaviors they always perform related to the android itself and their personal data. To make our questionnaire more reasonable and shorter, we got our questions using some reports and surveys for reference and found out the most relevant part to our topic. The detail of the questionnaire can be found from the URL: http://www.diaochapai.com/survey774663.

4 RESULTS ANALYSIS

4.1 Google & Open-source

With the spread of smartphone, things have certainly changed. Today, smartphone is a multi-function mobile communicated device rather than a traditional mobile phone. The hardware and the software of the smartphone are much more convenient and excellent. These extra features are great, but with the power they provide, there is also a threat. How to improve the security of the Android smart phone is a problem what the Google and smart phone manufacturer should face.

Nowadays, Android and iOS are used as the top two systems all over the world. Though there are many smart manufacturers chased Android, Android still face much more security problems than iOS. In all problems, fragmentation is always the vital one. And in my opinion, it was caused by open source. According to the definition of the open source from Wikipedia (Open Source. Wikipedia), when compared with others close source system, Android is cheaper and offers more space for every manufacturer to create its application. Because of these, Android was chased by many smart phone makers. However, all kinds of the products which made by the smart phone manufacturers are having the big problem - fragmentation.

4.1.1 Fragmentation of Android

Generally, the Android fragmentation problem means the terminal fragmentation and the system fragmentation. Fragmentation has caused so many problems, such as compatibility, and brought more loopholes for the system. For some examples, when a developer wants to popularize a new application, he needs to consider all Android platforms. This will cost so much time and money. Even worse, every platform will have its own loophole in the same application; Android version is updated in every few months. If the users do not update their version, then the company should fix the loophole in the old version because there are so many users who do not want to update their familiar version in the real life.

On the other hand, though the Google offers the Android market to encourage the developer to create some new applications. However, fragmentation makes Google not able to monitor whether the application is safe before it is downloaded by users. Every time, Google takes action after some users have got hurt, the “Whac-A-Mole” countermeasure is far not enough to protect customers of Android.

4.1.2 Root Authority

Root authority problem is another one which can be attributed to the feature of open resource.

Rooting is a process that allows you to attain root access to the Android operating system code. When you take your phone or tablet out of the box while there are plenty of settings you can tweak, you can only alter what the manufacturer allows you to. By gaining rooting access, it is free to customize the user interface, run services in the background and even replace system apps. As rooting allows you totally control your personal device in the level of operating system (Karch), it is not for everyone. Expertise users would like to enjoy its advantage and fun. Also, an increasing numbers of apps are now trying to help you on rooting.

However, rooted devices will expose high level of security issues. With the root access, a malware can do almost everything such as collecting sensitive information, making your phone call or surfing. It would be risky to put trust on a developers’ side and for most ordinary users (John), they even have no idea of what they can do or what have been done with your phone. Besides, it also violates the warranty and phone permanently served by manufactures or phone carriers. The Android system maintenance is no longer a default.

Google actually can do better to improve the current situation or at least make rooting process difficult. It is known that it is also a core reason why users prefer Android. Not universally, in Europe and US, it is legal to root the device. Therefore it is easy to find tons of applications in both Google Play store and other third party markets. Some suggest to close rooting access for users in the perspective of Google or mobile carrier while it seems impossible at this moment. All in all, the possible solution is trying to download any rooting software from official market instead of entrusted source and encrypting the personal data.

4.1.3 App Market Supervision

4.1.3.1 Threats

Android application market is the distribution platform for applications of Android an online electronics and digital media store (Google Play. Wikipedia). However, an increasing number of malwares published in the market are very active during past few years as Google loosens the control and application management mechanism. Although lots of anti-virus software can be downloaded and installed in the user's personal device, some measures are highly recommended to conduct before the malware has been successfully installed into the phone. One main issue that attracts much attention these years is the Google's supervision of its Android market. The verification processes for applications entering their market have been shown to be woefully and games being made legitimately available to users.

4.1.3.2 Popular Software Installation Model

a) The Walled-Garden Model

This model provides full control over third-party software installation on user's devices. Without the permission of a vendor, software cannot be released to a vendor's app market. Vendors are responsible to fully control the apps' security and testing before installed by users. In current market, iOS most resembles such model. Developers who wish to publish iOS apps have to submit to Apple for approval first. iTunes Apple Store will rejects apps that plug in malicious code or violate the intellectual property law.

b) The Guardian Model

In this model, the guardian is only responsible of the elementary of security decisions. It transfers its responsibility to a knowledgeable third party .It can be an app supervision organization or OS vendor itself or enterprise system administrator and so on. The vendor involves less than the first model, leaving most decision flexibility to the guardians. Users also minimally participate in decision making. For example, BlackBerry is belongs to this model.

c) The User Control-Model

The user in this model will have a highest level of participation of software installation as 3rd party apps are distributed without rigorous control. Android falls mostly into this model. Except for its official app market, other third parties' markets are also attractive to users and it is allowed to download an app from a website as well. It offers most flexibility to the users in customizing and apps selection.

The above three models display the level the system provider takes control of its application market. Obviously, comparing to iOS and BlackBerry, Android is minimally involved in the application supervision. Customers then will stand in a too risky situation as for most of the users, they totally trust the software providers, based on what hackers can easily plug malicious code into their apps and let it distribute and spread. We highly recommend Android to improve its control ability and make more efforts on restricting its application market. As its open source nature, it would be impossible to be like iOS, fully control over every third-party application. It may learn from BlackBerry. Having a RIM-approved app is beneficial and a plus for distribution purposes, unapproved apps can still be distributed outside the market. Android can start its application review process to some of software developers instead of all. Step by step, more app would like to join this approving process as an approved label which can be seen as a comparative competitive advantage in the app market. On the users' perspective, they are willing to choose software that has been reviewed and examined. Therefore, there is no certain model that we can say is the best. What we need is to find a more appropriate way for Android to convince its users.

4.2 Third-party Security Application

4.2.1 Experiment for 3D Magic Wallpaper

LBE vs. '3D Magic Wallpaper'

When '3D MW' is installed, LBE immediately detects that the application is over privileged to obtain user's location information. LBE warns user about the privilege escalation and provides with three permissions modes: "Allow" "Deny" and "Remind me". When '3D MW' is opened, the malicious ads automatically appear in the notification bar of the mobile phone but LBE cannot detect the malicious ads nor warn the user.

Lookout vs. '3D Magic Wallpaper'

When '3D MW' is installed, Lookout cannot detect the application is over privileged to obtain user's location information. On the contrary, Lookout identifies '3D MW' to be a safe application.

'360' vs. '3D Magic Wallpaper'

When '3D MW' is installed, '360' immediately detect that the application is over privileged to access to user's location information, turn on the Wi-Fi access, and obtain the mobile phone IMEI. '360' warns user about the over privileged actions and enables the user to allow, deny or remind when in use.

The malicious ads automatically appear in the notification bar when '3D MW' is opened, but '360' cannot detect the malicious ads and warn the user.

AVG vs. '3D Magic Wallpaper'

AVG can neither detect 3D MW is over privileged to access to user privacy nor discover the malicious ads.

Tencent vs. '3D Magic Wallpaper'

Upon the installation of '3D MW', Tencent can detect the application's stealthy access to obtain user's location information and IMEI but Tencent does not warn user of this immediately. At the very beginning, Tencent is unable to detect the malicious ads, but after the first time '3D MW' is run and the ads occurs, Tencent detects the malicious ads and adds it to the malicious actions list of '3D MW'.

4.2.2 Experiment for Truth or Dare

LBE vs. '3D Truth or Dare'

Upon the installation of 'Truth or Dare', LBE immediately runs a scanning on it and detects that the game is over privileged to obtain much user's private information such as user location. LBE warns user about the malicious permission and provides with three permissions modes. For the access to user location, if user selects the "Deny" option, LBE successfully denies the access to user location.

LBE detects the malicious ads immediately when 'Truth or Dare' is installed. LBE displays all malicious actions and plug-ins of the ads. When 'Truth or Dare' is opened, the malicious ads automatically appear on the screen, LBE successfully detects the ads and display an on-screen button with a cross sign to deny the ads. If the user selects the "Deny" option for ads, the ads are directly eliminated.

Lookout vs. 'Truth or Dare'

Lookout does nothing to 'Truth or Dare'

'360' vs. 'Truth or Dare'

Upon the installation of 'Truth or Dare', '360' immediately scans it and detects that the application is over privileged to obtain user's private information such as user location, and phone number. '360' warns user and provides with three permissions modes, which are "Allow" "Deny" and "Remind me". '360' successfully prevents 'Truth or Dare' from getting the user location information and the phone number. '360' also detects the malicious ads immediately when Truth or Dare is installed.

AVG vs. 'Truth or Dare'

After the installation of the game, AVG runs a scanning and detects that the game is a malware, AVG warns the users to uninstall it.

Tencent vs. 'Truth or Dare'

After the game is installed, Tencent immediately scans it and detects that the game is over privileged to obtain user location and the phone IMEI. Tencent warns user about the privacy violation and enables user to deny the unauthorized access. Tencent is also capable of detecting the malicious ads upon installation. Tencent displays all malicious actions and ads plug-ins, it enables user block the ads by setting, if user selects the “Block” option for ads, then ads are directly blocked and eliminated from the screen.

4.2.3 Experiment Results Analysis

	3D Magic Wallpaper		**Truth or Dare**	
LBE	Over privileged access to user location info	Y	Over privileged access to user location info	Y
	Malicious ads	N	Malicious ads	Y
Lookout	Over privileged access to user location info	N	Over privileged access to user location info	N
	Malicious ads	N	Malicious ads	N
360	Over privileged access to user location info	Y	Over privileged access to user location info	Y
	Malicious ads	N	Malicious ads	Y
AVG	Over privileged access to user location info	N	Over privileged access to user location info	/
	Malicious ads	N	Malicious ads	/
Tencent	Over privileged access to user location info	Y	Over privileged access to user location info	Y
	Malicious ads	Y	Malicious ads	Y

Table 2. The results summary of the experiment of third-party security application.

As shown in the experiment results summarization table, there are totally 20 observations (2 malware * 5 security apps * 2 malicious actions).

4.2.3.1 Commonality

In the experiment for ‘3D Magic Wallpaper’, most of the tested security applications cannot detect the malicious ads, for instance, although 360’s malicious ads defending mode is active; it still cannot detect the existence of the ads. In the experiment for ‘Truth or Dare’, majority of security applications can detect both over privileged access to user location info and the malicious ads. Comparing the two malwares horizontally, the performance of security applications on ‘Truth or Dare’ is obviously better that that on ‘3D MW’.

4.2.3.2 Individuality

LBE can detect the malicious ads of ‘Truth or Dare’, and it is a good practice that LBE displays an on-screen cross-sign button attached to the ads to deny the ads which is quite unique compared to others. Lookout is the only security application that does nothing to both two malware. ‘360’ is the only one to detect that ‘Truth or Dare’ is over privileged to obtain user phone number. AVG does nothing to ‘3D MW’, but it detects ‘Truth or Dare’ to be malware. Although AVG detects the game to be malicious, but it doesn’t specify what malicious actions the game entails, so the protection mechanism is coarse grained.

Tencent: Tencent is the only one that detects all malicious actions of the two malware. Interestingly, at the very beginning, Tencent cannot detect the malicious ads of ‘3D MW’. However, after the ads occurs when ‘3D MW’ is opened, Tencent detects the malicious ads and records it to the malicious actions list of ‘3D MW’.

4.3 User Behavior

After one week, 97 fully filled questionnaires were received and the answers of each question were found centralized on a few options.

4.3.1 Background

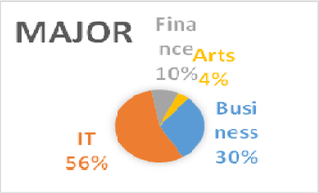


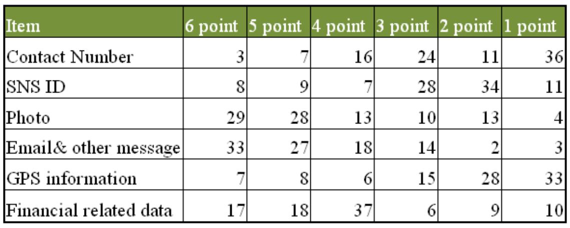
Figure 1. Major candidates

Because most of the respondents were from the SNS, we can see that the majority centralized in business and IT as shown in Figure 1. Information security is a hot topic in these two sectors we mentioned; therefore we can assume that our respondents would have more awareness and knowledge in this area than public users.

4.3.2 Security Awareness

The first one “Which option in your smart phone is the most important one due to your perspective?” is a ranking question; respondents will set a sequence from six information stored in their smartphone. The numbers show how many times the item is chosen. In order to assess the importance of each item, we gave 6 to 1 point to the rank 1 to 6 respectively and the table on the right side shows the results. Drawing lessons from the idea of assessing the risk, we calculated the weighted-average of each item based on the point and get the Table 3, which shows the final results for the first question.

We can now learn that for users, the top three important things are mainly private and sensitive information. Message contains the information about the daily life and private chatting of users. Photo has the content about users’ image. Financial related data will do harm to users’ money. Actually, according to Stevens (2012), these three types of data are all stored in our smartphone without any special protection and they are the main target of malicious apps. We can also see that, instead of focusing on financial related data, users pay more attention to the data about their daily-life privacy. Besides, the concern about some important data like GPS is relatively low. Therefore, we can learn that users’ awareness about security is always based on their common sense as shown in Table 4.



Item	6 point	5 point	4 point	3 point	2 point	1 point
Contact Number	3	7	16	24	11	36
SNS ID	8	9	7	28	34	11
Photo	29	28	13	10	13	4
Email& other message	33	27	18	14	2	3
GPS information	7	8	6	15	28	33
Financial related data	17	18	37	6	9	10

Table 3. Final results for the first

The second question is about the responsibility to protect the data. We found that all users believe google would take the responsibility to ensure security of their system. The reason varies from different individuals but the main thought is almost the same.

Users think they pay money to use the system for convenience, not for bringing them more things to concern and google as a businessman must ensure their product.

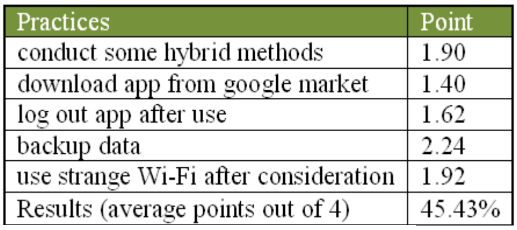
Item	Point
Email & other message	4.68
Photo	4.39
Financial related data	3.98
SNS ID	2.93
Contact Number	2.55
GPS information	2.47

Table 4. Ranking by importance

From these two questions, we can get the good news that users have built up some awareness to protect their personal data. Their concerns come mainly from their life experience and are not rational enough. What is more, users do not realize their obligation to protect their data when using Android devices.

4.3.3 Specific Behaviors

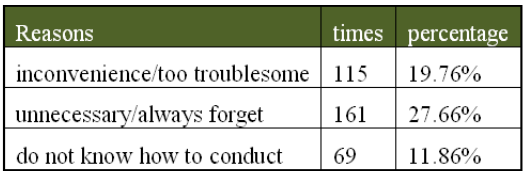
5 questions were set about good practices to test the frequency users perform them. Similarly, we assigned 4 to 1 points to the answer ‘always’ to ‘never’ respectively. We calculated the weighted-average for each practice. The number for each practice means the frequency the practice be done. The larger the number is, the lower the risk will be.



Practices	Point
conduct some hybrid methods	1.90
download app from google market	1.40
log out app after use	1.62
backup data	2.24
use strange Wi-Fi after consideration	1.92
Results (average points out of 4)	45.43%

Table 5. Users behavior

To find out the reasons for each behavior users chosen to be conducted, we use the statistic method to count the times each reason appear in our questionnaire. The results are showed in the tables 5 and 6.



Reasons	times	percentage
inconvenience/too troublesome	115	19.76%
unnecessary/always forget	161	27.66%
do not know how to conduct	69	11.86%

Table 6. Reasons

Table 5 shows that risk related to user’s behavior is quite high. Customers do not perform effective behaviors to protect their phones. The most common reason for the insufficient action is that they do not think taking so many steps to protect their smartphone is essential and they always forget to take the action. People also think taking the action is inconvenient even it will bring them too many troubles. Frankly speaking, most users give the convenience as the highest priority. They want technology make their life easier in not bringing more concerns. In summary, they do not realize the importance to improve the security for their smartphone, therefore they pay little attention to such area, making them feel it is troublesome and always forget the topic.

Besides, people always feel confusion when conducting behavior to improve the security for Android. For example, some respondents indicate that they know how to recognize the secure Wi-Fi and they cannot figure out how to back up their data.

5 DISCUSSION

5.1 Google & Mobile Carrier

For Google, as the top developer of the android market, open source is a competitive strategy more than a development mode. Google wants to earn more money; the open source may be the best choice. If Google restricts the Android as much as the Apple does, the smart phone manufacturers may chase the other system and the application developers will do so. As a result, if Google wants to keep its market share, the open source will be insisted without stopping.

However, Google still cannot ignore the fragmentation. The best way to solve this problem is updating Android's version more slowly, and regulate the smart phone manufacturer with a strict regulation. Such as formulating the appropriate standard for each product. Though it may cause some manufacturers leave the Android platform, it can bring more benefits for Google in the future.

Otherwise, if Google always focus on its market share, then the fragmentation will become a huge obstacle in front of the compatibility forever. Without the consistency between the system and the device or hardware, the compatibility cannot be guaranteed. Finally, fragmentation will cause the compatibility of Android device worse and worse. The only result is because the difficulty of the development on Android platform is increasing, all the manufacturers and apps developers will leave Android, and this classical system will fail at last.

Every move of the third-party manufacturers which consist of the hardware producers and applications developers will have a direct influence on every single aspect of Android system. Every smart phone manufacturer wants its product safer and with less loopholes than other products. In all kinds of security measures which are offered by manufacturers, there are two ways what I recommend is most useful.

5.1.1 Appropriate one is better than new one

There are so many manufacturers chasing to provide new applications for their users. They pay much attention to how new/cool application is and how many Android platform it can match. However, they usually ignore what the users need.

Nowadays, we can easily find there are so many unknown applications in our Android smart phone. Even till we buy a new phone in the future, there are some applications we never use or aware of. Actually these useless applications often contain some malicious software or loopholes, such as "Charging Malpractice". This malicious software can collect your private information or make you have to pay the bill unconsciously. Then, the first thing to do is so many Chinese users who buy a new Android smart phone is running the RUU (ROM Update Utility) to exclude the potential threats.

As a result, it is easy to create a new application for users, but it is hard to create an appropriate application who can meet the demanding of the users, and this is what we should focus on.

5.1.2 Improve the security precaution for existing function

Generally, there are two purposes on the theft of smart phone. One is for the information which is stored in our phone (Open Source Security 2008). By the comparison, we can find that Android smart phone manufacturers still need to improve the security level of their products.

SD card is a benefit or a threat?

> "An SD Card (Secure Digital Card) is an ultra-small flash memory card designed to provide high-capacity memory in a small size. SD cards are used in many small portable devices such as digital video camcorders, digital cameras, handheld computers, audio players and mobile phones." (Secure Digital. Wikipedia)

In order to enhance the memory capability of the Android smart phone, manufacturers offer the interface to SD card. Android system supports the application of SD card but without any security mechanism for it. If someone picks up our Android smartphone and he wants to get the important information we stored in the SD card, he just needs to pull it out from our phone and combine it with some PC hardware, then all the information can be read completely. This loophole is very dangerous for the business man. In this respect, iOS does a good job. At first, iOS does not support SD card application, so there is no security problem in this area.

Who should judge the requirement of escalation allowance?

On the other hand, iOS has a few privilege escalation allowance mechanism. In contrast, Android is full of this mechanism. It seems that Android provides a higher security mechanism for our phone. In fact, this mechanism does not work as we expected because this mechanism is based on the skill level of the user. Usually, common users find the convenient way to get the application. They spend money for enjoying the application but making judgments. For example, we go into a barbershop, we just want to choose the service it provides but we do not want to judge which tool the barber should use! So many users ignore the threat of these requirements of escalation allowance, actually. Moreover, if the application is defined to be trustworthy, then all the security mechanism will move away. we think this is a horrible loophole.

In conclusion, we think the Android system is designed by a series of excellent thinking. However, there is still a long way for it to perfect its security mechanism.

5.2 Third-party Security Applications

5.2.1 Current Security Applications Analysis

We can draw several conclusions based on the experiment results.

Firstly, the effectiveness of the protection of mobile security and user privacy by Android security application vary from malware to malware, which is probably due to the individualities of different malwares. Some malwares are made by more powerful hacking language, thus increasing the difficulty for security tool to detect and defend.

Secondly, for one identical malware, the effectiveness of different security applications varies from each other substantially. In the experiment, for one malware, some security applications can detect all malicious actions violating user privacy, and provide user with tackling methods while some security applications do nothing to the malware. This outcome can be easily reasoned that different security tools have different security technology set and expertise. For instance, AVG even doesn't contain the module of application permissions monitoring and management, thus the efficacy of securing the user privacy is weak.

As a whole, the effectiveness of Android security applications in protecting mobile security and user privacy is not as optimistic as we anticipated. One of the respondents is the user of Android security application; he thought that as long as the security tool was installed on the phone, he would be definitely free of security threats and violations. However, the experiment significantly changes his original perspective, the experiment tells us that security tools is not all to secure mobile security and user privacy, without user awareness and utilization of the tools, the effectiveness of the security applications is substantially downgraded compared to that they are anticipated to be.

5.2.2 Suggestions for Third-party Security Applications

First of all, as the experiment is initiated to help us find inspirations to recommend security application developers. From the experiment, the maliciousness of the malwares is obviously seen and we believe that the destructiveness of malware is more severe than what we observed in the experiment. Android security application developers should make effort in security technology innovation. The velocity of security technologies innovation should resolve the upgrading speed of malicious technologies so that user privacy can be well secured.

Secondly, the standalone Android security application cannot take the entire task to secure user privacy. What matters is user awareness of information security and the collaboration with security tools. Unluckily, the actual situation is that majority of Android users have weak awareness and the security functions are badly utilized by users. Therefore we recommend security application developers to take user interaction into consideration to refine the functions or user interface. For instance, the application can be more aggressive in tackling malwares; for some very dangerous malwares, the application can block the application and inform user the dangerousness. Instead of simply telling user what to do for malware, the application can illustrate the danger of malicious actions by additional text warning or visual warning.

The user's important role to be aware of information security and to utilize and collaborate with security applications inspires us is to investigate on user's awareness and behaviors for Android security, which will be discussed in the following session.

5.2.3 Limitations of the Third-party Application Test

Firstly, the experiment pool is small which inherently affects the accuracy of the experiment. Since the experiment only samples 2 malwares and 5 security applications, the sample size is below the optimal sample size.

Secondly, apart from the limitation of sample size, the configuration of the sample is another drawback, which means the selection of security applications, malicious applications, and selection of mobile phone. Since we did not acquire sufficient and integrative knowledge of Android system security, we can hardly design an optimal configuration of the experiment sample that can generate optimally accurate results. Our selection of the experiment subjects is based on our historical observation and use experience of mainstream Android security, malicious apps and the mobile phone.

Thirdly, the observation is the result variable of the experiment and greatly affects the accuracy of the experiment. In our experiment, the variables are to see whether the effective detection can be observed which is a simple observation variable and limits the accuracy of experiment. The observations design can be further improved by observing some quantified variables, such as the number of malicious actions detected by security tools.

Fourthly, the experiment is lack of a quantitative analysis to empirically interpret the results, however the quantitative study can only be applied to big sample size that our experiment doesn't satisfy.

5.3 User Behavior

It is both Google's and users' responsibility to make efforts to improve the security for Android as well as our smartphone. Users are always not experts in IT area, therefore Google must use methods to guide the users' behavior. In order to achieve the secure goal from the aspect of user, two directions are suggested.

5.3.1 Improve user's awareness of security

Because the awareness of security is quite low, making the users treats the security activity as unnecessary; Google must take steps to improve the users' awareness. One suggestion is to indicate the severe threats by an interesting and vivid video when Android was firstly launched. The content should focus on every aspect of Android security especially the data which was considered not so important as personal privacy like GPS information or the contact number. After knowing the threats to their data as well as smartphone, users will have the motivation to take action to control these risks.

5.3.2 Provide the best practices and assist user to conduct

We suggest Google should first provide the best guideline to users for following. For example, customer should not download app from the third-party market because the external apps are not under Google’s control or they should backup their data in case of any accident. In order to assist user well conduct such action, we suggest Google set a mechanism. The mechanism can appear when there exist threats and can provide some related advice to customer. Besides, in some circumstance, the system can provide some auxiliary tools like app for analyzing whether the free Wi-Fi is secure. By doing so, customer can get the direction and the essential information to conduct security behavior.

6 CONCLUSION

This paper has examined the security of Android platform from three different aspects, which are Google and mobile carrier, third-party security and user behavior. According to the results shown from the Google’s perspective, Android has a bunch of problems needed to be solved by the joint effort of Google and hardware manufacturers. Similarly, the effectiveness of Android security applications in protecting mobile security and user privacy is not as optimistic as expected. Therefore, besides the measures should be taken by Google and the third-party security application developers as well as hardware manufacturers, users need to be trained to change their certain kinds of behaviors. Users should be well-advised to increase their awareness of security and certain practices and assistance can also be performed by Google for the sake of improving the security knowledge base of Android users.

7 REFERENCES

Avancini, A. & Ceccato. M. (2013). Security Testing of the Communication among Android Applications. Automation of Software Test.

Barrera, D. & Oorschot, P.V. (2011). Secure Software Installation on Smartphones. IEEE Security & Privacy, vol. 9, no. 3, pp. 42-48, May-June 2011, doi:10.1109/MSP.2010.202.

Berger, B.J., Bunke, M. and Sohr, K. (2011). An Android Security Case Study with Bauhaus. Reverse Engineering (WCRE), 2011 18th Working Conference. pp 179-183. ISSN: 1095-1350.

Bing, H. (2012). Analysis and Research of System Security Based on Android. Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference pp 581-584. ISBN: 978-1-4673-0470-2.

Breitinger, F., & Nickel, C. (2010). User Survey on Phone Security and Usage. BIOSIG 2010 -- Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, pp. 139-144.

Framingham, M. (2013). Android Pushes Past 80% Market Share While Windows Phone Shipments Leap 156.0% Year over Year in the Third Quarter, IDC. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS24442013.

Google Play. Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/Google_Play.

Jeter, L. & Mishra, S. (2013). Identifying and Quantifying the Android Device Users' Security Risk Exposure. Computing, Networking and Communication (ICNC), 2013 International Conference. pp 11-17, doi:10.1109/ICNC.2013.6504045.

John A. What is Rooting on Android? The Advantages and Disadvantages. [Online]. Available: http://droidlessons.com/what-is-rooting-on-android-the-advantages-and-disadvantages/.

Karch, M. Why Do People Root Android Phones? And What is Rooting? Google. [Online]. Available: http://google.about.com/od/AndroidPhonescat/qt/Why-Do-People-Root-Android-Phones.htm.

Miler, C. (2011). Mobile Attacks and Defense. IEEE Security & Privacy, vol. 9, no. 4, pp. 68-70, July-Aug. 2011. doi:10.1109/MSP.2011.85.

Pieterse, H. & Olivier, M.S. (2012). Android Botnets on the Rise: Trends and Characteristics. Information Security for South Africa (ISSA) 2012. pp 1-5. ISBN: 978-1-4673-2160-0.

Secure Digital. Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/Secure_digital_card.

Shan, P. (2010). Mobile Internet More Popular in China than in U.S. The Nielsen Company. [Online]. Available: http://cn.en.nielsen.com/documents/ChinaMobileReport.pdf

Stevens, R., Gibler, C., Crussell, J., Erickson, J. & Chen, H. (2012). Investigating user privacy in android ad libraries. In Workshop on Mobile Security Technologies (MoST).

Open Source Security (2008). The Government of the Hong Kong Special Administrative Region. February 2008

Open Source. Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/Open_source.