Underlying Factors Influencing Security Performance

GROUP 5:

Raditya Arief
Eren Celik
Ana Guerra
Luigi Tuttobene

In our previous assignments, we have considered the variance in security performance in relation to our metrics (malware detection ratio, malware presence ratio, and malware download ratio) and how different risk strategies among actors can shape this variability. In this report, we aim to explore the underlying reasons or factors, behind the variance in security performance of the actors involves in the security issue. In the first section, we discuss the different strategies followed by market owners, customers, application developers, and even attackers to mitigate (or foster) the impact of malware in Android applications. For do so, we identify a concrete countermeasure that actors involve in the security issue could use in order to mitigate its impacts. Then, we analyze the distribution of cost and benefits among the different actors if adopting the countermeasure. After that, we investigate whether the actors involve the security issue have incentives to take the countermeasure. Lastly, we study the role of externalities in this context. In the second section, we chose the Android application market because its security performance is visible in our metrics. We identify different factors that could explain the variance in the security performance. Then data of some of this factors is collected by desk research. After that, we perform a statistical analysis to explore the impact of the factors in our metrics. Finally, some conclusions are derived from this assignment.

Part I: Actors and Relationships

1.1 ACTORS

1.1.1 Market Operator

The perspective of the market owner has detailedly been investigated in the previous assignment. In particular, we have analysed cost and benefits of the Android Vulnerability Reward Program introduced by Google in 2015. Despite the imprecision in our measurement, we are confident about the positive results of such programs. As a matter of facts, similar projects has been developed for years with the same aim on different platforms, computer programs in primis.

Its positive effect on Android security has already been acknowledged on Google Online Security Blog. (2016). In its first year, the program has rewarded researchers with more than $550.000, and the investment has increased by 33% this year.

Despite we believe that this strategy will not increase Google's competitive advantage, as it is easily imitable by competitors, we identify three critical factors for its successful implementation:

- the reward might be a limitation: many small companies might not afford these expenses;
- the number of users: a larger the customer base results in a higher number of *bug-hunters;*
- setting up costs are limited (almost irrelevant for google, affordable for smaller markets like Baidu or 360).

Advantage: ideally the cost is proportional the effective number of issue solved.

Perspective of other actors:

It is an efficient solution against attackers, as similar programs address the problem of zero-day vulnerability exploit.

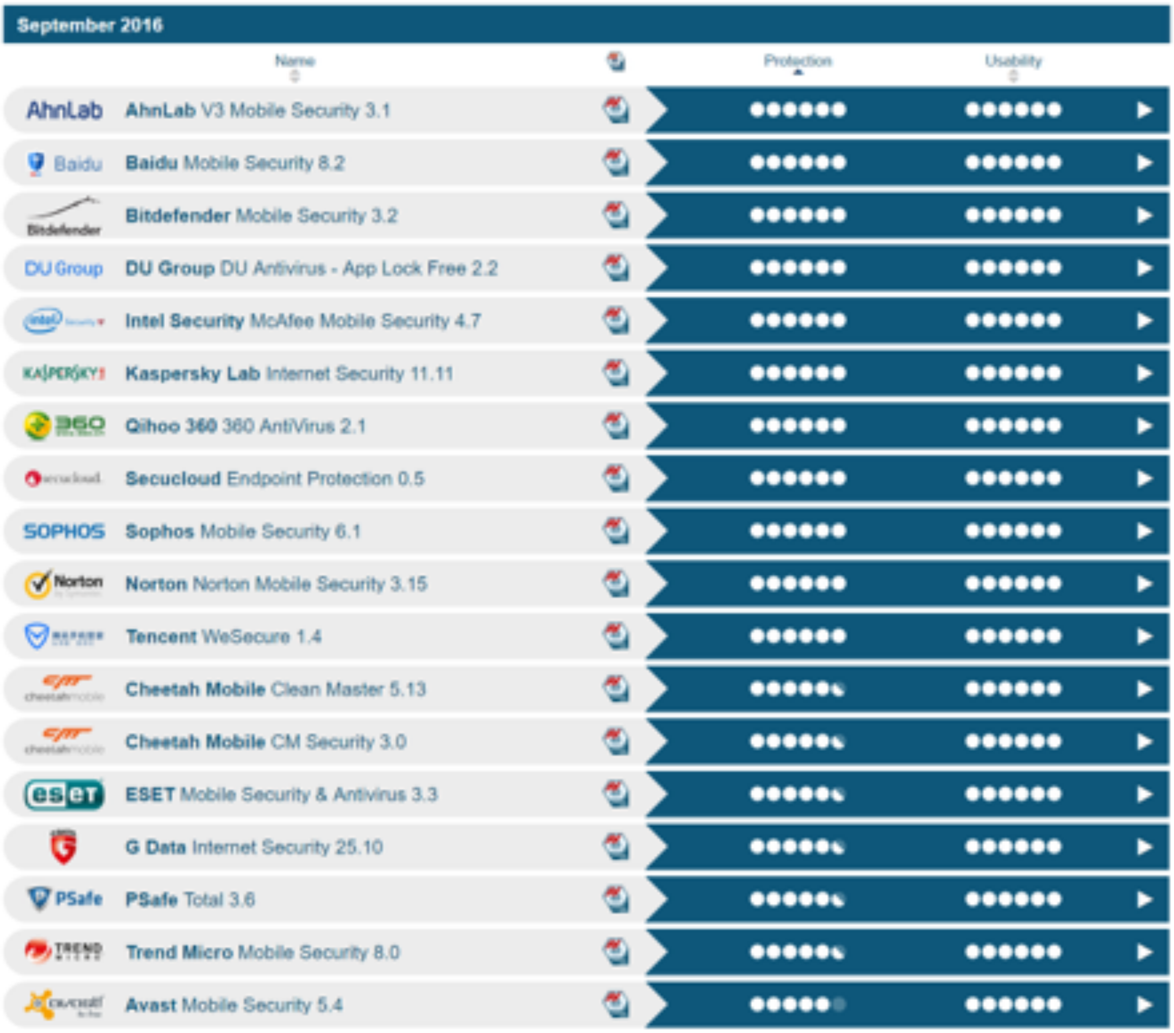
App developers would enjoy the result of the program as free riders. Surely, they can contribute to the success of the program by establishing alliances and sharing resources. However, they can also enjoy positive externalities, free riding the security brought by the program.

For the final user is an interesting solution. It might work as awareness campaign as well, increasing the level of brand loyalty.

1.1.2 Customer

There are different countermeasures that application users can undertake to mitigate the presence of malware, and thus its terrible consequences, in their devices. One the most rational/recommended actions is to download applications from reputable, sources such as the official Android application store, only. According to Google Android security review, Google play has the lowest rate of malware infection and the company constantly works for enhancing its security performance (Google, 2015). However, as we know, not all consumers have access to official application markets, this is the case for China, where Google and all it services were blocked in mid-2014. Therefore, this is not an option for the Chinese application consumers.

The second option is using mobile antimalware, generally known as mobile antivirus, for android devices to mitigate the infection risk. Antivirus (anti-virus) is a software program that prevents, detects, and remediates malware infections on individual computing devices. The name antivirus was originally given to programs that identified and removed a particular type of malware called virus. However, nowadays, antivirus are utilized for preventing infections caused by different type of malware such as worms, Trojan horses, rootkits, spyware, keyloggers, ransomware and adware (Rouse, 2005).



September 2016

Name	Protection	Usability
AhnLab V3 Mobile Security 3.1	●●●●●●	●●●●●●
Baidu Mobile Security 8.2	●●●●●●	●●●●●●
Bitdefender Mobile Security 3.2	●●●●●●	●●●●●●
DU Group DU Antivirus - App Lock Free 2.2	●●●●●●	●●●●●●
Intel Security McAfee Mobile Security 4.7	●●●●●●	●●●●●●
Kaspersky Lab Internet Security 11.11	●●●●●●	●●●●●●
Qihoo 360 360 AntiVirus 2.1	●●●●●●	●●●●●●
Secucloud Endpoint Protection 0.5	●●●●●●	●●●●●●
Sophos Mobile Security 6.1	●●●●●●	●●●●●●
Norton Norton Mobile Security 3.15	●●●●●●	●●●●●●
Tencent WeSecure 1.4	●●●●●●	●●●●●●
Cheetah Mobile Clean Master 5.13	●●●●●◐	●●●●●●
Cheetah Mobile CM Security 3.0	●●●●●◐	●●●●●●
ESET Mobile Security & Antivirus 3.3	●●●●●◐	●●●●●●
G Data Internet Security 25.10	●●●●●◐	●●●●●●
PSafe Total 3.6	●●●●●◐	●●●●●●
Trend Micro Mobile Security 8.0	●●●●●◐	●●●●●●
Avast Mobile Security 5.4	●●●●●○	●●●●●●

Figure 1. Most common AV software

Using mobile antivirus applications involve two main actors: mobile antivirus application vendors and consumers. As we saw in Economics of Security, edX edge videos, there are not incentives for vendors to come up with better products than the competition. Therefore, they prefer to invest money in marketing and promoting activities rather that in enhancing the malware detection capacity of their products.

Customers, on the other hand, are able to choose between different antivirus alternatives. AVTEST, an independent IT-Security Institute, provide monthly information about the best antivirus software for Android. The institute classifies vendors according to antivirus protection (detection of the latest Android malware in real-time, detection of the latest Android malware discovered in the last 4 weeks), usability (performance regarding battery use, slowing down devices, traffic generation; and false warnings), and special features.

The cost of antivirus applications goes from monetary charge such as monthly fee (2.01 EUR for AhnLab), yearly fee (14.56 EUR for AhnLab), lifetime license; to no monetary or free of charge (Baidu, 360 Security, DU Group). However, the latter, specify that the application contains ads or consumers need to pay certain premium actions. Although only users can decide to buy an antivirus application or to deal with ads in free antivirus apps, the highest cost that users paid is to give access to all data, information, applications, search engines, and device capabilities to an application for being safe.

Among the benefits of mobile antivirus applications, the best mobile antivirus applications offer not only malware detection and prevention, but also a range of privacy and anti-theft features that include the ability to back up contacts and other data, track phones or tablets via GPS, snap a picture of a phone thief with the device's camera, and even use Android Wear smartwatch to locate user's phone (Tom's Guide Staff, 2016).

Some criticism of mobile antivirus applications is first, signature-based antivirus scanners, which efficiently detect known malware, have serious failures with new and unknown malware. In addition, malware developers test their application using the most popular antivirus application. Second, unlike desktop antivirus software, mobile antivirus have resources limitation on mobile devices. Furthermore, mobile operation systems impose restrictions to those applications. Finally, the rapidly growing number of mobile application is outpacing the industry's ability to analyze, catalog, and construct the signatures necessary for identifying embedded viruses and malware (Li & Clark, 2013).

Consequently, there are doubts regarding how effective is the use of antivirus in mobile devices, and there is not supported evidence that shows a decrease in the security issue due to antivirus. However, customers who perceive that the benefits overweight costs will have the incentive to use antivirus as a countermeasure.

1.1.3 App Developer

There are several countermeasures that the app developers can pursue. One of those countermeasures is to apply secure software development life cycle. In brief, secure software development life cycle prompts software developers to implement security best practices at each stage of its software development process. Secure software that is up to the highest standard is achievable by following the latest best practices. Most of the times, the owner of each software platform would provide guidelines and documentations describing what security features available and which best practices to follow to achieve the highest security level as possible.

The cost and benefits are one interesting perspective to look at in the issue of secure software development. The benefits of secure software will be perceived by the users. On the other hand, the implementation of security best practice will not only incur benefits but also costs to the app developers. The costs of secure software development include the longer development time and the necessity to hire qualified programmers.

Does the benefit secure software development will outweigh the cost from the app developers' perspective? The answer might be yes and no. For the big and famous IT companies that have already secured a share of the market, the benefits of secure software development arguably outweigh its costs. However, for the smaller IT companies, also called startup companies, the outcome might be quite different. This difference can be attributed to one of the impacts of network effect to the IT industry; the fastest company to gain the majority of market share has a substantially higher chance of becoming the market leader. Therefore, these startup companies often sacrifice app security for faster deployment time. In brief, depending on the condition of the company, the secure software development practice can be either beneficial or detrimental.

Looking at the costs and benefits analysis of implementing secure software development countermeasure from the app developers' perspective, it can be understood why most app developers, at least in the beginning, have a very weak incentive in implementing it. The secure software development practice not only incurs costs but also brings minimum benefits to the app developer. The longer software development time may cost the company the chance of becoming the market leader. Moreover, in such case where there is any adverse consequence happened caused by the lack of security, the actor that will bear the biggest loss usually is the users, not the app developers. Looking from this perspective, however unethical it might be, the implementation of this countermeasure is unattractive for most app developers.

The security issue in app development reflects an apparent externalities issue; the lack of effort to secure applications by the developers will likely inflict harmful consequences to the app's users while it imposes insignificant to almost none impact to the developers themselves.

1.1.4 Attacker

The attacker has a different dynamic when it comes to strategies. The attacker strategies in the case of app-markets involve evading detection. Be it hiding malware from preemptive scans to evasion analysis by emulation/sanboxing this is also known as dynamic analysis.

Unique malware code is safe from conventional malware scans. It becomes more challenging when heuristics come into play. With dynamic analysis it becomes possible to analyse the behaviour of an app over time. It is here where even (original) code can be caught. So it is imaginable that most well hidden malware will be picked up at the emulation/sanboxing stage. Thus a good strategy is to evade detection under emulation.

Dynamic analysis will alert for any suspicious behaviour. Malware programmers have two options in trying to evade detection. Stall or detect. By stalling any malicious action is delayed for an extended period. This is done in hope that the dynamic analysis lasts shorter than the stalling period. This is hard to implement as the clock of a system can be emulated and fast forwarded as well in hope of uncovering stalled malware. If the malware stalls too long it will also not be as effective as it possibly could be. The other option is that the malware is able to detect that it is in an emulation. Once it detects this it will only engage in benign processes. This detection can be relatively easily implement by checking for various information like device names, product numbers, sim card information, operator name, APIs, etc (source). Currently attackers and defenders are in a constant arms race in this field (source).

For the attacker it is fairly easy to implement detection techniques. Especially since such attackers can be very well organized businesses. It takes time and effort indeed to take part in the arms race. "Compromising a method is only one vulnerability away." On to of that, techniques can quickly spread amongst attacker groups and organizations. An attacker can of course greatly benefit from such strategy.

Defenders are in a constant process of improvement. They can never know what vulnerability will be (ab)used next and are therefore in a constant reactive battle. This battle is constant because it is the most important front. This reactiveness can be costly because when malware makes it through it infects many devices. Knowing the predominant reactive nature of this fight means that malware will evade it, infect devices and ultimately turn a profit for the attacker. On the defenders end remediation can be expensive and damaging to the brand name. Depending on how well an attacker can keep evasive code secret from other attackers it will have a longer lifecycle. Also if the attacker is dependent on how vigilant a user base is. If users are quick to flag apps as suspicious then it becomes increasingly harder to stay undetected. The effect is that the code has a much shorter lifecycle and will force the attacker to find another way to stay undetected.

1.2 Externalities

In this section we investigate the relations among actors, explaining their dependencies and trying to show how the harmonious growth of Android ecosystem is related to these relations.

1.2.1 Features of Android Ecosystem

The growth of the system is a delicate issue: as the system grows in size (number of users and applications) and its interdependencies become more complex, so do the answers to the security challenges. Moreover, due to a larger installed base, it becomes more attractive to attackers;

Action/ Externalities	Actors in Android Application Markets				
	Market owner	Application Customers	Applications developers	Attackers	Remarks
Market owner implements an Android Vulnerability Reward Program to provide monetary rewards for vulnerabilities disclosed	*Market owner takes the action that creates a positive externality.*	*Customers have more incentives to download app from that particular market. Moreover, customers also have incentives to search for vulnerabilities.*	*App developers have less incentives to spend time and money searching for vulnerabilities in their app. Someone will figure out and report the vulnerability. They will put their efforts just to repair the app.*	*Attackers have incentives to buy vulnerabilities information for third parties.*	
Market owner heavily invest in security for their platform As a result, app markets free of malware.	*Market owner takes the action that creates a positive externality.*	*Customers have incentives to download app from secure markets. However, they do not have incentives to invest in antivirus protection anymore.*	*App developers have incentives to create better applications less vulnerable.*	*Attackers have inceptives to find we ways of spreading malware in Android devices.*	
Customers relying on mobile antivirus application to protect their devices. As a result, less malware spread among users.	*Market owner end up having less incentives to make security investments because customers are taking care of their security.*	*Customers taking actions that creates a positive externality.*	*Mobile antivirus app developers have more incentives to create better products (efficient to detect malware) which are more appealing to customers.*	*Attackers have more incentives to create new types of malware which will not be detected immediately by antivirus app.*	*Example of network externalities in cybersecurity. To be effective the countermeasure, the majority of/all customers should follow it.*
Customers downloading apps only from reliable sources. As a result, less fraudulent places with malware.	*Market owner has more incentives to ensure security to customers because they aim to be a reliable source for customers.*	*Customers taking actions that creates a positive externality.*	*App developers have more incentives to develop more secure applications because they also aim to be considered as a reliable source.*	*Attackers have more incentives to infect reliable sources with their malware. A huge impact can be achieve in this way.*	*Example of network externalities in cybersecurity. To be effective the countermeasure, the majority of/all customers should follow it.*
App developers applying secure software development cycles. As a result, app will be ensured with best practices at each stage of its development	*Market owner will have less incentive to invest in security. However, they do have incentives to create better best practice guidance.*	*Customers have more incentives to download app.*	*App developers taking actions that creates a positive externality.*	*Attackers have more incentives to infect app even though apps developers follow best practices.*	*Example of network externalities in cybersecurity. To be effective the countermeasure, the majority of/all customers should follow it.*
Indirect intermediary liability from regulatory parties can also lead to externalities.	*According to the severity of regulation, market owners could have incentives to leave the market if their profitability is affected.*	*Customers have no incentives to care about security if they know that market owners will cover any damage due to malware infections in the market*	*App developers can be hold liable also for this regulation, therefore they could have incentives to follow best practices requirement by markets*	*Attackers usually are beyond the reach of law in this cases thus, they do not have incentives to change its behavior.*	

Table 1. Externalities in Android ecosystem

Android ecosystem is build on the foregoing mentioned relationships among four actors. Their cooperation against attacker is crucial to the harmonious growth of the system. In such an interdependent environment it is hard to assess to which extent any observation might be considered the outcome of a particular action. In

other words, evaluating cause-effect relationship is complicated due to these interconnections. This affect the distribution of benefits as well as the one of costs.

Moreover, the strategies each actors can pursuit to consolidate security can affect positively to the security of the whole system: this means that the other parties would free-ride benefits of such measures, which is called positive externality. Positive externalities bear issues to information security because people or firms involved in the transaction do not capture the full benefits therefore they undervalue the transaction. On the other hand, third parties can also be imposed with harm due to other parties actions, which is call negative externalities. Table 1 shows how externalities due to actors' actions influence the incentive of other actors.

Examples:
(1) User is infected by a ransomware. The cost are payed by the user, and only indirectly by the market operator;
(2) User is infected by a botnet, with the aim of launching a DDoS attack against a third party. Here the heaviest consequences are payed by the third party (negative externality).

It is in general, it is true that app markets are characterised by network externalities. As a matter of facts, the value of an application increase with the number of users. This is particularly true for messaging applications like WhatsApp or social media like Facebook, for sharing-economy-oriented app like AirBNB or BlaBlaCar, and for many other productivity and financial applications. However, this also implies that actions to pursue security will only be effective if more user implement the same security actions.

The security within the system is affected by information asymmetry. This is particularly manifest in the case of AntiVirus software. App developers, in fact, have more information about their product compared to the users. (two lines more?)

Lastly, an important factor that steer security in this environment is related to what we can call time to market. Most of the software on an mobile market, in fact, come from small companies. Startups who enter the market have heavy budget constraints: security investments in early stages of development, where the survival of the company depends on the rapid diffusion of the application, are not attractive. However, there will be a moment, sooner or later in the life cycle of the company, in which investments in security will be preferred over the development of new features.

1.2.2 Reflections about Interdependencies

I) The use of mobile antivirus will improve users security, detecting attackers traps. However the market of antivirus is heavily affected by information asymmetry. Moreover, many AV vendors might find attractive to lead the user in a lock-in. A good example here is McAfee computer program. Many PCs were sold with McAfee preinstalled as default antivirus. Despite the (in)efficiency of the software itself, the aspect of interest was the impossibility to uninstall the package, forcing the user to continuously update the software.
As last remark about the AV market it is interesting to notice that there are many customised solutions, where the user authorises the AV vendor to collect data to improve the service. On the flip side of the coin, the vendor might use these data for different purposes. (…a bit more?)

II) At the same time, the diffusion of antivirus apps has a positively impact not only to the security of the environment but also to its growth.

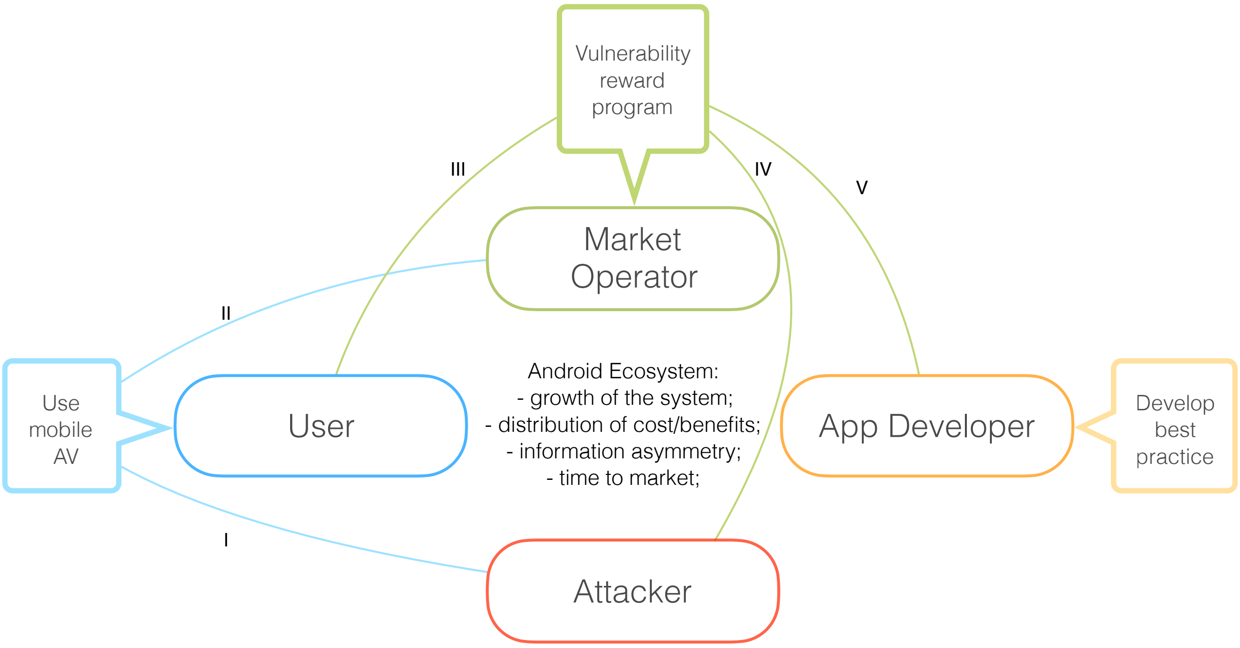


Figure 2. Security strategies and effects.

III) Projects similar to Android's Vulnerability Reward Program will have definitely an effect on users, as they would be actively involved in security dynamics. Moreover, since the cost of such program can be seen proportional to their efficiency, for the market operator they represent an attractive strategy to secure the market and to brace customer loyalty.

IV) An interesting feature of Android Vulnerability Program is its impact on attackers. These programs, in fact, address the problem of the black market for vulnerabilities (…2 lines more?)

V) App developer would get benefits from these programs as free-riders: without effort (surely they can however contribute) they will take advantage of a securer environment.

Actors involve in the security issue can take different countermeasures to mitigate the presence of malware in Android markets and android devices. For instance, market owners can invest on security implementing Android Vulnerabilities Reward Programs, which offer a monetary compensation to vulnerabilities discoverers. Customers can download content only from reliable sources, and use mobile antivirus applications to avoid malware infections. And application developers can ensure that best practices at each stage of development have been followed. However, actors applying countermeasures to mitigate the security issue can create positive externalities. As a result, any action that produces a positive externality to other actors ends up diminishing the incentives of these other actors to take additional measures to avoid the security issue. In addition, many security countermeasures present network externalities, which means that the security action works only as more people adopt it.

Part 2: Statistical Analysis

2.1 Collecting Data of Factors

The section above has defined the factors that possibly correlate with Malware Presence Ratio. The information about these factors is usually not available directly but rather need to be derived from an entirely different source of information. Sometimes, this effort also requires several assumptions. This section will describe the data used for the correlation analysis, how the data was derived, and the assumptions made for the derivation.

We have designed the a causal model as a starting point of our analysis, and deriving the following hypothesis.

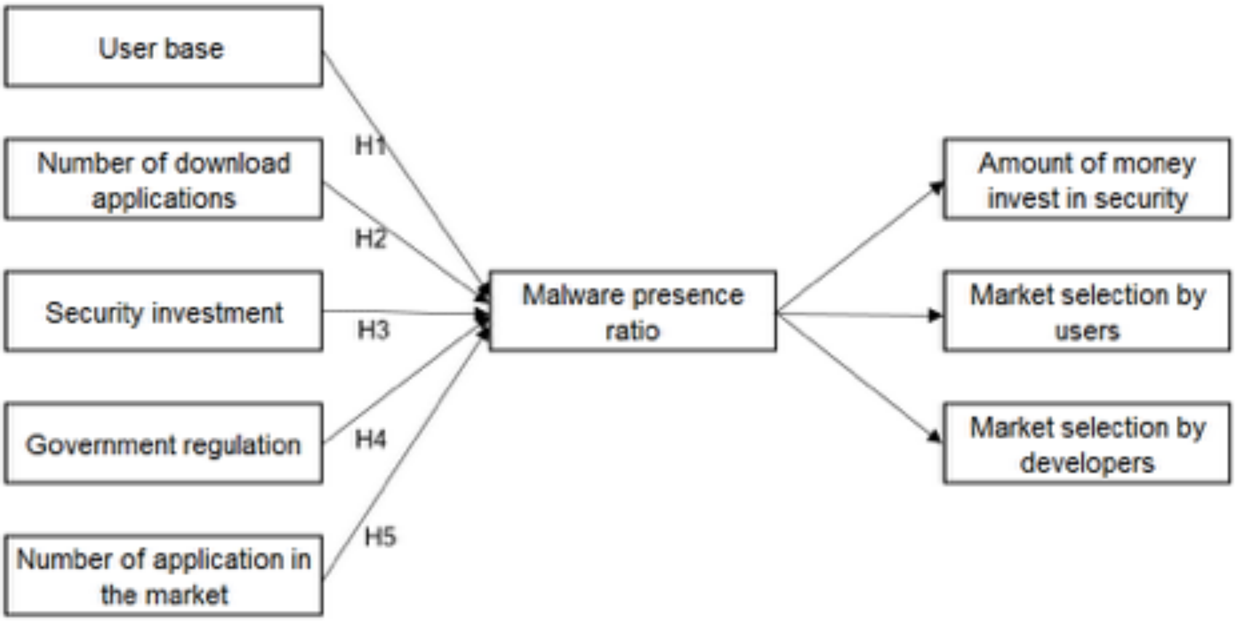

User base
Number of download applications
Security investment
Government regulation
Number of application in the market
H1
H2
H3
H4
H5
Malware presence ratio
Amount of money invest in security
Market selection by users
Market selection by developers

Figure 3. Causal model at the base of the analysis

H1. The most users a market have, the highest the malware presence in the market.
H2. The higher the number of download app, the higher the malware presence in the market.
H3. The highest the security investment, the lowest malware presence in the market
H4. Strong government regulation against malware correlates positively with low malware presence in the application market.
H5. A high number of applications in the market correlates with a high malware presence in the market.

2.1.1 User Base

The User Base factor is simply the number of users use the service of this app marketplace. This data is one of the rather straightforward data that do not require derivation process or any assumptions. The User Base data of Baidu, Qi Hoo 360, and Google Play are presented in Table 2 below.

Market	User Base	Market Share
Baidu	> 165 million	8.1%
Qi Hoo 360	> 275 million	13.5%
Google Play	> 1 billion	71.4%

Table 2. User Base and market share data

There are many contesting statistics. Numbers differ wildly among the different sites. The interesting thing is that statistics generating companies like https://www.talkingdata.com/ are exactly "stolen" data is used for. User base information is of 2016 unlike the other statistics which originate from 2014.

2.1.2 Number of Download

The number of download of each marketplace corresponds to the average number of daily downloads in a certain period of time. For example, the number of download of Baidu in 2014 can be calculated by dividing the number of total download from Baidu marketplace in 2014 by 365. The Number of Download for each marketplace can be seen in Table 3.

Market	Number of Download
Baidu	> 60 million
Qi Hoo 360	> 170 million
Google Play	> 200 million

Table 3. Number of download

The lack of straightforward information about the number of download require the data in Table 3 above to be calculated from two information sources. First, it is informed that the percentage of number of download for Qihoo 360, Tencent Myapp, and Baidu are 42.6%, 34.6%, and 25.5% respectively (CIW Watch, 2016).

Second, it is also reported that Tenscent mobile appstore had daily distribution of 110 million (Cecilia, 2015). From these data, the download numbers for Baidu and Qi Hoo 360 can be calculated.

2.1.3 Security Investment

It was impossible to determine Cyber Security budgets for all companies. So instead, the revenue and company profile is used to estimate a number. According to Cecilia (2015) spending median ranges from 3% to 5% but average is less than 3%. Depending on business strategy, vision and industry the budget can be anything between 0.3 -15%. From this assumption the Cyber Security budget is calculated.

Market	Revenue	Cyber Security Budget
Baidu	$1.39 billion	$97 million
Qi Hoo 360	66.38 billion CNY ($9.80 billion)	$980 million
Google	$74.54 billion	$5.22 billion

Table 4. Security budget

For medium to large organizations, the number swings between 7%-9%. Baidu and Google being a huge tech company with a wide expertise is projected to spend 7% on Cyber Security. In contrast 360 is projected to spend 10% of the budget on IT and about and at least 10% on Cyber Security since it is a Cyber Security company.

2.1.4 Government Regulation

Government regulation is one of the potential contributing factors to security performance. However, it is also difficult and tricky to come up even with least reliable data. Although it is difficult to develop a metric for government regulation in each country, as it turns out it is equally difficult to gather information about these regulations. Because of these difficulties the correlation analyses will not be done for this factor. Nevertheless,

2.1.5 Number of App on the Market

Number of apps offered in each market share can also potentially be a contributing factor. However, our team encountered problems with finding the information about number of apps for Baidu and Qi Hoo 360. The information for Google can easily be found, but it was not the case for the other two markets.

2.2 Correlation Analysis

In the previous submission, our team has developed a security metric for these application markets. This metric is called malware presence ratio. In short, the malware presence ratio is the percent of all collected apps that are detected as malware. The malware presence ratio of all markets can be seen in Table 5. In this section, the data of each factor gathered in the previous section will be analyzed using linear regression to conclude whether a strong correlation exists between each factor and the malware presence ratio metric.

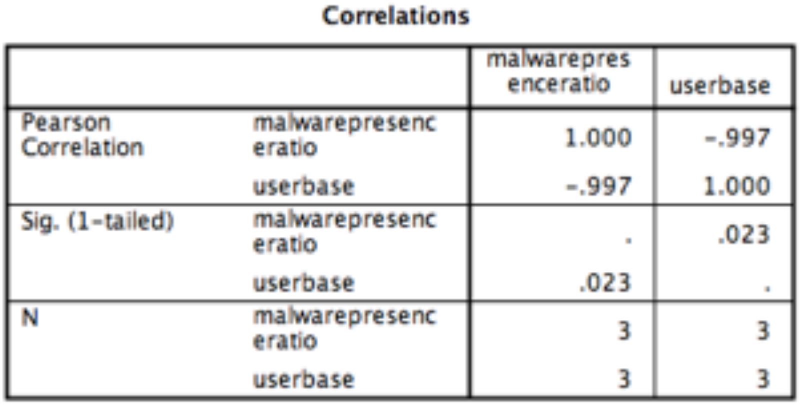
Market	Malware Presence Ratio
Baidu	59%
Qi Hoo 360	47%
Google Play	0.1%

Table 5. Malware presence ratio of each market

The IBM SPSS Statistic software is used to run the linear regression analysis. In the results provided by SPSS, the attention will put to Correlation table and ANOVA table. It worth remembering that the analysis done in this report is correlation analysis, not the causation analysis. It means that if in such case where high correlation is found, it does not necessarily imply that both factors are related in such cause-and-effect relationship.

2.2.1 User Base

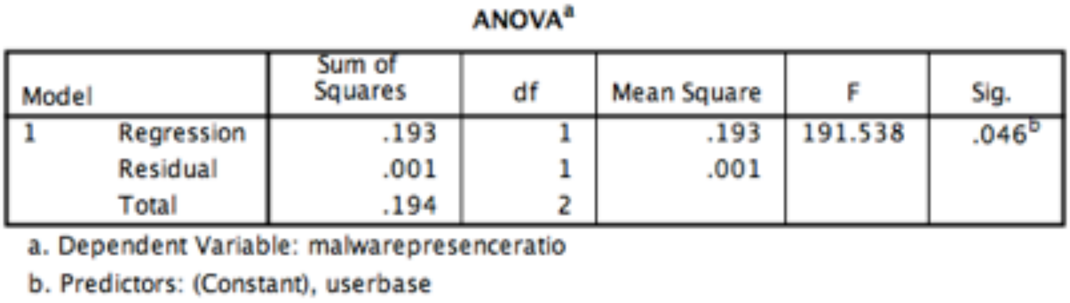
The analysis result for user base factor can be seen in Table 6 and Table 7. The results from the SPSS show that this factor has a high negative correlation. This result means that the bigger the user base, the lower is the malware presence ratio. The result contradicts the H1 hypotheses. Moreover, the significance level in the ANOVA table shows that this result is statistically significant.



Correlations

		malwarepresenceratio	userbase
Pearson Correlation	malwarepresenceratio	1.000	-.997
	userbase	-.997	1.000
Sig. (1-tailed)	malwarepresenceratio	.	.023
	userbase	.023	.
N	malwarepresenceratio	3	3
	userbase	3	3

Table 6. Correlation Table of User Base



ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.193	1	.193	191.538	.046[b]
	Residual	.001	1	.001		
	Total	.194	2			

a. Dependent Variable: malwarepresenceratio

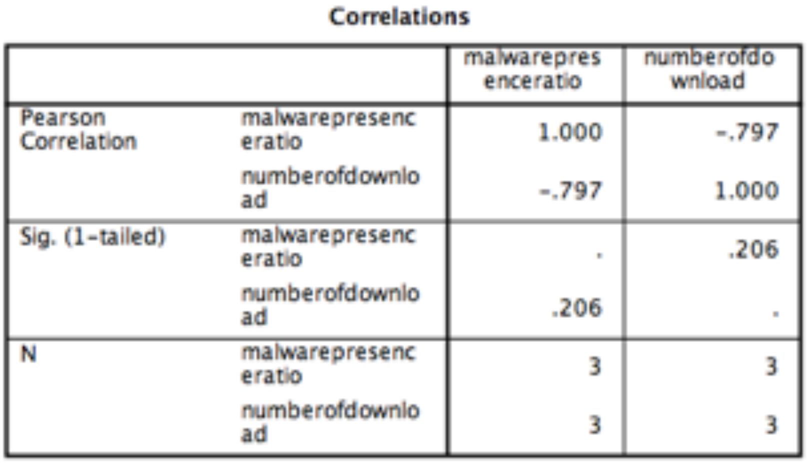
b. Predictors: (Constant), userbase

Table 7. ANOVA Table of User Base

There might be some explanation to this result. The rationale behind the H1 hypotheses was that the bigger market is more attractive to attackers. As the results show this is not the case. One of the possible explanations is that companies with bigger user base has already enough budget to invest in security, hence the negative correlation.

2.2.2 Number of Download

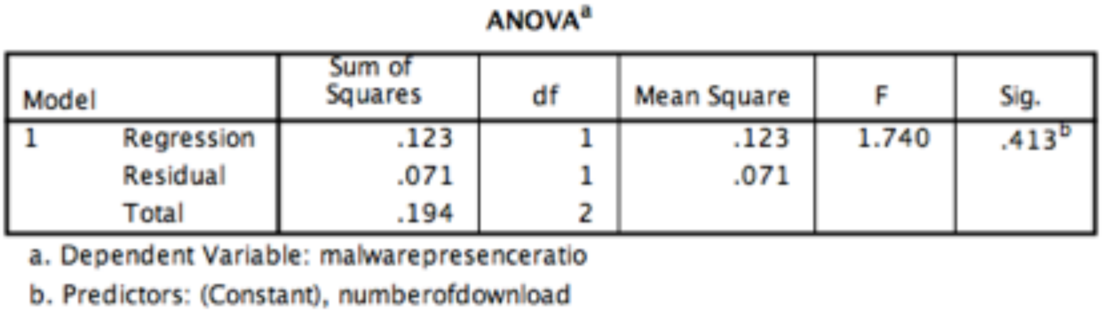
The statistical analysis results for number of download can be seen in Table 8 and Table 9. Although the correlation analysis shows a quite strong negative correlation, but the significance level is not statistically significant.



Correlations

		malwarepresenceratio	numberofdownload
Pearson Correlation	malwarepresenceratio	1.000	-.797
	numberofdownload	-.797	1.000
Sig. (1-tailed)	malwarepresenceratio	.	.206
	numberofdownload	.206	.
N	malwarepresenceratio	3	3
	numberofdownload	3	3

Table 8. Correlation Table of Number of Download



ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.123	1	.123	1.740	.413[b]
	Residual	.071	1	.071		
	Total	.194	2			

a. Dependent Variable: malwarepresenceratio

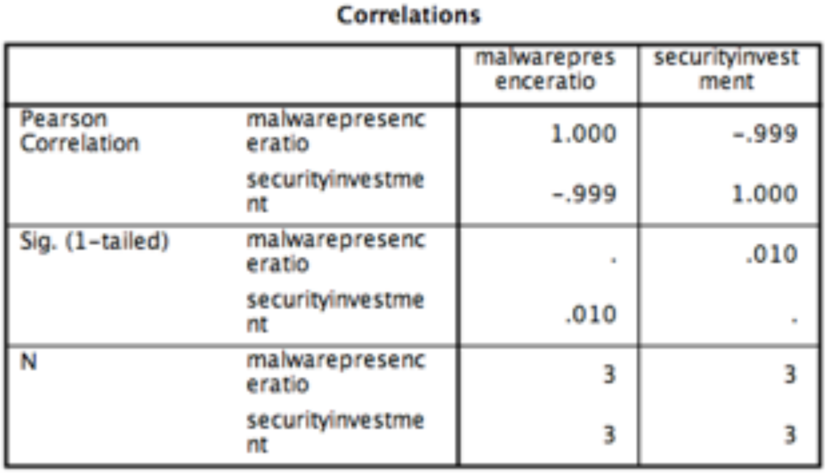
b. Predictors: (Constant), numberofdownload

Table 9. ANOVA Table of Number of Download

It is quite hard to explain these findings because the lack of data. The Baidu and Qi Hoo 360 serves a market from which the Google Play is banned and the Chinese market itself contributed to 59% of all app downloads in 2014 (Kan, 2015). So it would be tricky to come up with any conclusion based only on these findings.

2.2.3 Security Budget

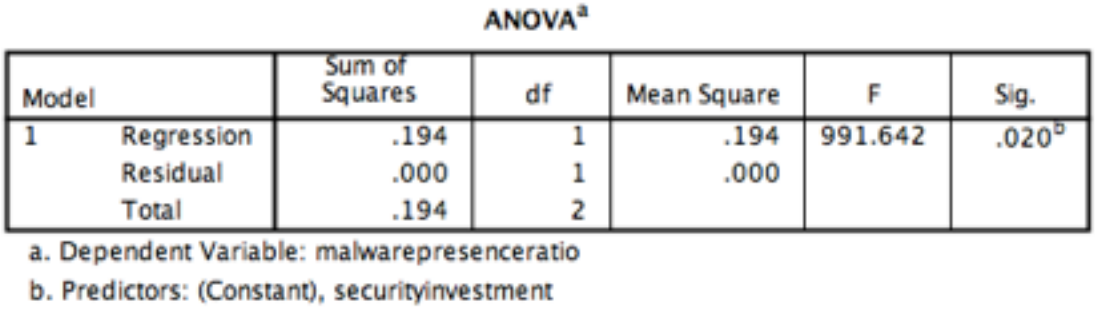
The security budget is the last factor analyzed for this report. From the correlation table, it can be seen that the security budget factor represents a very high negative correlation; the higher the security budgets the lower the malware presence ratio. Moreover, the ANOVA table shows that this factor is statistically significant with p-value of 0.020.



Correlations

		malwarepresenceratio	securityinvestment
Pearson Correlation	malwarepresenceratio	1.000	-.999
	securityinvestment	-.999	1.000
Sig. (1-tailed)	malwarepresenceratio	.	.010
	securityinvestment	.010	.
N	malwarepresenceratio	3	3
	securityinvestment	3	3

Table 10. Correlation Table of Security Budget



ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.194	1	.194	991.642	.020[b]
	Residual	.000	1	.000		
	Total	.194	2			

a. Dependent Variable: malwarepresenceratio

b. Predictors: (Constant), securityinvestment

Figure 11. ANOVA Table of Security Budget

Although these findings show significant and high correlation, they do not imply anything about causation. Still, it is perfectly make sense to argue that security budget determines the security performance. More data and deeper statistical analysis might be able to describe the relation between security budget and malware presence ratio further.

2.3 Conclusion

In the second part of this report, the role of market owner in influencing the security issue, which is depicted by the malware presence ratio in a software marketplace, is elaborated further. Some factors that potentially explains the variance in the malware presence ratio are defined. The factors are the size of user base, number of applications downloaded from the marketplace, the security investment/budget, the government regulation, the number of application offered in each marketplace. These factors then analyzed to see if they correlate with the malware presence ratio. However, because of the lack of data, the government regulation and the number of application factor in the market cannot be taken for correlation analysis.

The result of the correlation analysis is quite interesting. Both the size of user base and the security budget are statistically significant factors and highly correlated with the malware presence ratio. On the other hand, the number of downloads neither statistically significant nor highly correlated. Some possible explanations for these results have been described. Although it is difficult to gather further conclusion beyond these correlation analyses, such as defining possible causation, more data and information about marketplace accompanied deeper statistical analysis might yield more meaningful and richer conclusion.

References

Cecilia. (2015, January 5). 70% App Downloads From Mobile App Stores in China. Retrieved October 23, 2016, from China Internet Watch: https://www.chinainternetwatch.com/11705/70-app-downloads-from-mobile-app-stores/

CIW Watch. (2016, June 9). China Android App Stores Insights Q1 2016. Retrieved October 23, 2016, from China Internet Watch: https://www.chinainternetwatch.com/17661/android-app-stores-q1-2016/

Filkins, B. (2016). SANS Institute InfoSec Reading Room. SANS Institute.

Google. (2015). Android Security: 2015 Year in Review, (April), 1–43. Retrieved from https://source.android.com/devices/tech/security/reports/Google_Android_Security_2014_Report_Final.pdf\nhttp://googleonlinesecurity.blogspot.com/2015/04/android-security-state-of-union-2014.htm

Google Online Security Blog. (2016). One Year of Android Security Rewards. [online] Available at: https://security.googleblog.com/2016/06/one-year-of-android-security-rewards.html [Accessed 31 Oct. 2016].

Kan, M. (2015, February 25). With no Google, Chinese app stores soar on high downloads. Retrieved October 23, 2016, from PC World: http://www.pcworld.com/article/2888892/with-no-google-chinese-app-stores-soar-on-high-downloads.html

Li, Q., & Clark, G. (2013). Mobile Security: A Look Ahead. IEEE Security & Privacy, 11(1), 78–81. http://doi.org/10.1109/MSP.2013.15

Monica, G. (2015, August 27). What You Need to Know About App Distribution in East Asia. Retrieved October 23, 2016, from OneSky Blog: http://www.oneskyapp.com/blog/asia-app-distribution/

Newzoo;. (2016, August 1). TOP 10 ANDROID APP STORES | CHINA. Retrieved October 23, 2016, from Newzoo Website: https://newzoo.com/insights/rankings/top-10-android-app-stores-china/

Rouse, M. (2005). Definition: antivirus software. Retrieved October 22, 2016, from http://searchsecurity.techtarget.com/definition/antivirus-software

Tom's Guide Staff. (2016). Best Android Antivirus Apps 2016. Retrieved October 22, 2016, from http://www.tomsguide.com/us/best-antivirus,review-2588-7.html

Vincent, J. (2015, September 29). Android is now used by 1.4 billion people. Retrieved October 23, 2016, from The Verge: http://www.theverge.com/2015/9/29/9409071/google-android-stats-users-downloads-sales

Woods, B. (2016, January). Google Play had twice as many app downloads as Apple's App Store in 2015. Retrieved October 23, 2016, from The Next Web: http://thenextweb.com/apps/2016/01/20/google-play-had-twice-as-many-app-downloads-as-apples-app-store-in-2015/