Mobile Advertising Security Risk Assessment Model Based on AHP

Jing Li[1], Hui Fei[2],Wei Jin[1]

[1]*Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 10029, China;*

[2]*Beijing University of Posts and Telecommunications, Beijing, 100876, China*

Abstract

As the proliferation of mobile malware advertising, there are no existing industry rules and legal restrictions on them, users need to identify and undertake adware risk by themselves. In response to this situation, it puts forward mobile advertising security risk assessment model based on AHP. This model refers to industry standards, mobile Internet malicious code description specifications and the large number of mobile advertising sample results, dividing risk into privacy disclosure, flow-consuming and hooliganism three risk factors and assessing risk factors and their relative importance of sub-factors. Based on AHP theory calculating the risk factor weights, it solves the problem for assessing the risk of malicious ads. Finally, it actually analyzes the risk level of mobile advertising in mobile applications and validates the model is feasible.

Keywords: mobile advertising, analytic hierarchy process, privacy disclosure, hooliganism

Introduction

Mobile advertising is the mobile marketing mode of devoting the information of promotion or brand from advertisers to mobile applications (App). Application advertising operators achieve massive advertisings and managements by building the advertising SDK plugs in the mobile applications, so that the developers' user flows can become the advertising revenue.

But for the more targeted advertising some advertisers don't hesitate to steal user privacy and even some add malicious code that can implement hooliganism behaviors, for example downloading software in the background to the ads for malicious deductions. According to the 360 Mobile Security Testing Center, there are more than one billion malware advertising in over China's 70 million Android phones Intercepted by the 360 mobile guards. The applications bundled with malicious adware have an installed capacity of over 247 million people. It means that the phone of one in the Android phone users of the country has been infected by malicious adware and at least infracted 14.3 times for the past four months [2].

Faced with threats of mobile advertisings' grim situations, the country's security vendors introduced a series of ad-blocking and detecting engine, for example Kingsoft for mobile phones, Tencent mobile phone guard, LEB security master, 360 mobile guard. The detecting engine primarily focus on the discovery of mobile malware adverting, lacking risk assessment of mobile advertising, so that the users can not identify the risk of advertising exactly. In addition, the different standards of assessment by different security companies also lead to the same batch of mobile applications' detection results have large gaps that can cause distress to the users. Therefore, based on the unified standard, detailed and comprehensive evaluation of mobile advertising security risk is very important.

1 Risk classification

At present, each of malicious mobile advertising evaluation standards of the each company is not the same. The "four standard" of Qihoo 360's mobile malware advertising include anonymous pushing, unable to close, forced downloading, malicious deductions. Kingsoft's define of the ads are coming from unknown sources, no disclosure or unable to clear the notification bar advertising, stealing user privacy, malicious deductions and frequent popping. According to specification for mobile Internet malicious code, it can be found that both standards are too sample and do not take into account some factors ,for example Qihoo 360 standards do not involve user privacy, modifying equipment information and other malicious acts, Kingsoft' standards ignore forced background downloading. Therefore, this paper based on specification for mobile Internet malicious code, combined with Qihoo 360 and Kingsoft’s standards and, classifies the risk of mobile advertising, mainly includes privacy disclosure, flow-consuming and hooliganism three categories.

1.1 Privacy disclosure

We randomly selected sample of 57 001 applications from the application stores, analysis adware codes and obtain the statistics of privacy disclosure caused by mobile advertising, in which 27,376 applications do not contain advertising, 29,625 applications use more than 55,000 times advertising. Most of these mobile ads obtain user privacy [3] and upload them to the remote server behavior in the background. Privacy disclosure is mainly reflected in these aspects, reading device serial number, reading device identification number, reading the position information [4], reading text messages, reading the address book, reading a machine phone number, reading the log, reading the list of installed applications [5]. The distribution situations of these privacy disclosure behavior of specific mobile advertising are shown in Figure 1.

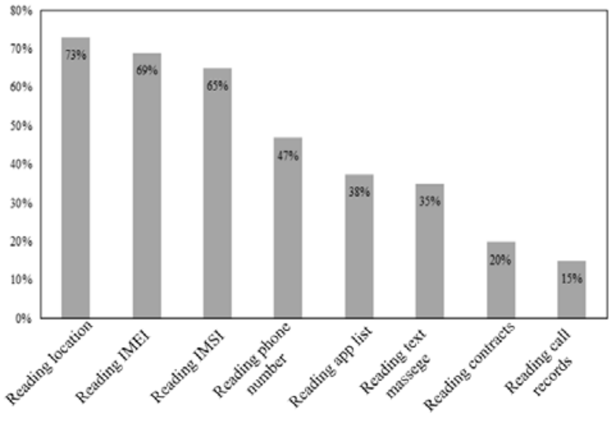

Figure1. privacy disclosure about mobile advertising

1.2 Flow-consuming

Mobile advertising flow-consuming is mainly in three aspects, pushing ads or video full screen, background downloading software, frequently updating advertising. In order to study the flow-consuming of mobile advertising, we use official advertising platform SDK to simulate 11 ads which push ads to cause flow-consuming, specifically in Figure 2. We found that some adware including Baidu, Youmi, Adchina push full-screen, video advertising, which spend 100KB ~ 1MB flows per hour and that frequently updated advertising platforms including Mango, WAPS, appjoy on average spend about 2.4MB flows per hour. These adware on average update every 30 seconds, which means that the adware' updating once consumed an average of 20KB flows. How much flow Background downloading software spend depends on the size of installation package. The current installation package size is generally between 500KB ~ 25MB, and the most is nearly 10MB. Therefore, the background downloading software most affects the flow-consuming.

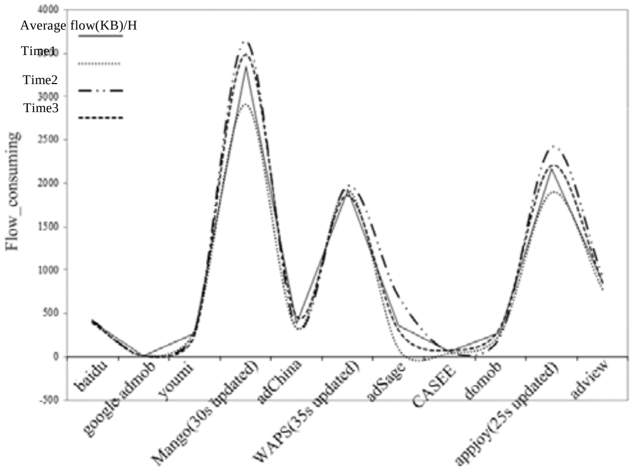

Figure2. flow-consuming about mobile advertising

1.3 Hooliganism

Hooliganism is the other malicious behavior which has no direct damage to the system, is not harmful for the users' personal information and charges [6], including anonymous forcibly pushing ads, advertising which cannot be closed, and modifying device information.

- Anonymously forcibly pushing the advertisements

Some application developers take advantage of Android's notification bar functions to forcibly push the advertisings. When a user opens the application or his phone is in the standby state, the forcibly pop-up ads will guide the user to click to download other applications. Because users cannot confirm which application is the source of the advertising, they cannot finally block the ads by promptly uninstalling the applications.

- The advertisements unable to close

Users can not turn off some advertisings which violate the rights of the user's choice and affect the user experience.

- Modifying the device information

Such as creating a desktop shortcut, adding an icon, modifying browser settings.

2 Risk assessment model

Based on mobile advertising risk classification, to establishing evaluation model, shown in Figure 3. Model has the target layer, the first criteria layer, the second criteria layer. To calculate the risk factor weights, you first need to assess the first criteria layer, the relative importance between risk factors for the second criteria layer and users.

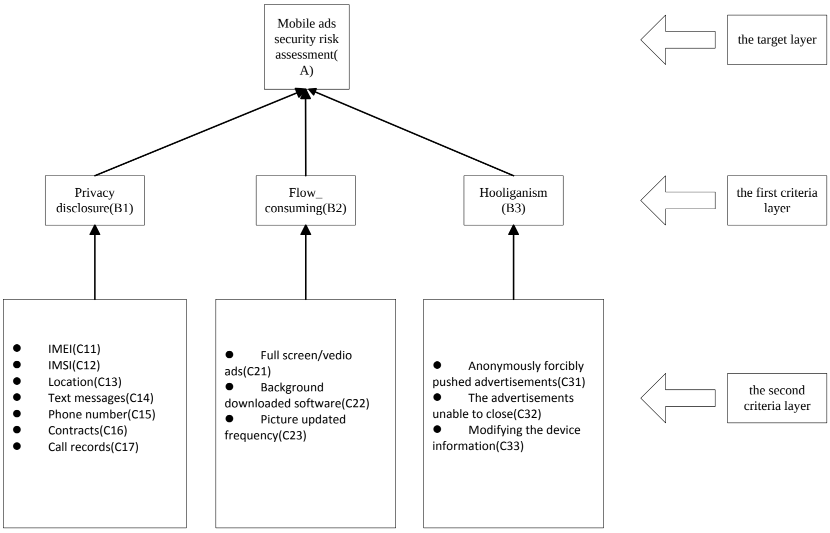
Mobile ads security risk assessment(A)
the target layer
Privacy disclosure(B1)
Flow_ consuming(B2)
Hooliganism (B3)
the first criteria layer
● IMEI(C11)
● IMSI(C12)
● Location(C13)
● Text messages(C14)
● Phone number(C15)
● Contracts(C16)
● Call records(C17)
● Full screen/vedio ads(C21)
● Background downloaded software(C22)
● Picture updated frequency(C23)
● Anonymously forcibly pushed advertisements(C31)
● The advertisements unable to close(C32)
● Modifying the device information(C33)
the second criteria layer

Figure3. mobile advertising security risk assessment model

2.1 The first criteria layer risk factor

2.1.1 The first criteria layer risk factor

Privacy disclosure in most cases is to study user preferences, in order to better advertise or push information to the user. Flow-consuming takes a direct result of user charges consumption. Hooliganism has no direct harm to the users, but it will affect the users' experience. According to 1-9 comparison scale, based on these three elements relative degree of influence on the user's assessment of their relative importance, It assumes hooliganism slightly significant impact on users, and show that privacy disclosure is obviously important and flow-consuming is strongly important. The factor vector of privacy disclosure, flow-consuming and hooliganism impacting on mobile advertising is $B = \{ 5, 7, 3 \}$.

2.1.2 The Second criteria layer risk factor

- Privacy disclosure factor

Based on the principles of importance whether the factors can cause direct losses, indirect losses about privacy, we assess the relative importance of privacy disclosure factor. We assume that IMSI and IMEI are normally important, whose relative importance value is 2. Therefore, the list of installed applications involving users' favors, is slightly more important than formers, whose relative importance value is 3. The location disclosing users' tracks is obviously important, whose value is 5. The phone number, contacts, text messages, phone records are mightily important, whose value is 9. Therefore, the privacy disclosure factors including IMSI, IMEI, location, text messages, phone number, contacts, call records, reading the list of the installed applications ,whose relative importance vector is $C_1 = \{2,2,5,9,9, 9,9,3\}$.

- Flow-consuming factor

Full screen ads or video ads generally cost 10KB ~ 500KB flows. Frequently updated ads spend about 2.4MB per hour. Due to the different application sizes, a size of the software background downloaded generally can achieve trillion level, and the time required is much less than one hour. According to three kinds of flow-consuming, to set the vector which indicates the relationship between full screen or video ads, background downloading software, images updating frequency and the flow-consuming is $C_2 = \{3,7,5\}$.

- Hooliganism factor

The behavior of unable to close advertisings can block ads by closing the application. Anonymously forcibly pushing the advertisements needs to determine the source of the advertisements, which is less likely to block ads. Therefore, the latter is slightly more important than the former. The behavior of modifying the device information is in the background, which is not easy to detect by users. Therefore, it is a little more important than the behavior of unable to close advertisings. The vector about the influence between these three factors and hooliganism is $C_3 = \{2,1,3\}$.

2.2 Calculating risk factor weights

The steps based on Analytic Hierarchy Process, according to the importance of vector B, C_1, C_2, C_3 establish judgment matrix, and find the right level of single sorting criteria that heavy layer characteristic roots by law. To set the first criteria layer' weight W_i = {0.3333,0.4667,0.2000}, the second criteria layer' weight W_{1j} ={0.0417,0.0417,0.1042,0.1875,0.1875,0.1875,0.1875,0.625}, W_{2j} = {0.2000、0.4667、0.3333}, W_{3j} = { 0.3333、0.1667、0.5000}, to verify single-level sorting consistency. Finally, based on the total level of ordering principle $W_{ij} = W_{i1} * W_{1j} + W_{i2} * W_{2j} + W_{i3} * W_{3j}$, to seek the second criteria layer of mobile advertising security risk assessment's weight W_{ij} ={0.0139, 0.0139, 0.0347, 0.0625, 0.0625, 0.0625, 0.0625, 0.0208, 0.0933,0.2178,0.1556,0.0667,0.0333,0.1000},to verify meeting consistency test, indicating that the model is feasible.

2.3 Model application

Using linear weighted method gives the degree to be detected malicious advertising function, namely

$$R = \sum_{i=1}^{3} \sum_{j}^{n} W_{ij} P_{ij} \tag{1}$$

W_{ij} is the advertising risk assessment weight. P_{ij} represents whether the j-th sub-factor of the i-th factor on the first criteria layer exists.

$$P_{ij} = \begin{cases} 0 & The\ malicious\ behaviors\ do\ not\ have\ the\ decision\ factor \\ 1 & The\ malicious\ behaviors\ have\ the\ decision\ factor \end{cases} \tag{2}$$

Through a lot of analysis for the experimental samples, we determine the extent of malicious mobile ad index as shown in Table 1.

Table1 malicious mobile ad index

A	[0,0.2]	(0.2,0.35]	(0.35,1.0]
Malicious Level	Low risk	Intermediate risk	High risk

3 Analyzing experiment results

In order to verify the reliability of the mobile adverting security Risk Assessment Model, about 30 applications, selected from the Android store, were analyzed to detect security engine and manual analysis, and 19 softwares were found containing adware. By Using the Model, a risk assessment of these 19 software adware were taken, and compared with the assessment of security vendors. The result is that, evaluation results only contained two kinds of security vendors: recommend treatment or optimization and no risk. The experimental results compare with the results is high risk and low-risk model assessment.

As standard of security vendors engine evaluation is not unified, the detection results are different. In order to ensure the accuracy of the results, Tencent mobile phone steward, Golden hill poison bully mobile phone, 360 Mobile Phone Guardian were selected to compare. The result is showed in figure 4, The abscissa a0~a19 refers to the 19 softwares that the safety evaluation model and engine contains ads plugin, according to the compared result from the figure 4 samples can be found that the results of the assessment model is very comprehensive, including high risk, intermediate risk and low risk. The result of the detection engine Evaluation is simple and different. But the six applications which have high risks according to the detection of the assessment model are suggested to improve by at least one detection engine. The remaining four intermediate-risk applications and eight low-risk applications are assessed as risk-free applications by the security engines. On the whole overall, the results based on the assessment model are nearly the same as the detection engines', which are more comprehensive and easy to identify.

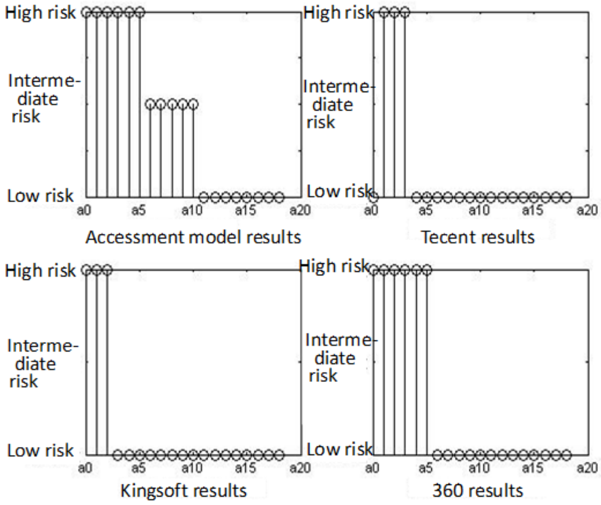

Figure4 sample contrast result

4 Conclusion

This paper presents a security risk assessment based on AHP mobile advertising model, and use the model to assess the application on the market, through the test results by mobile security engine to verify the accuracy and comprehensiveness of the assessment model. But the analytic hierarchy process itself is characterized by subjective evaluation results which may lead to high false positive rate. And with the emergence of new mobile advertising impact factor, the model also needs to be optimized and can be adapted by considering the application of neural networks, Bayesian networks, machine learning and other methods in future work.

5 Acknowledgment

Wei Jin is the corresponding author of this paper. This work was supported by a grant from the National Key Technology R&D Program (No. 2012BAH45B00).

References

[1] Iresearch. *2012 China Mobile application advertising platform Research Report*.(2012-09-17), http://report.iresearch.cn/1769.html.

[2] 360. *China intelligent mobile phone malicious advertising management report*.(2012-09-26), http://bbs.360safe.com/thread-37544-1-1.html.

[3] Grace M C, Zhou W, Jiang X, et al. *Unsafe exposure analysis of mobile in-app advertisements*, Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2012: 101-112.

[4] Stevens R, Gibler C, Crussell J, et al. *Investigating user privacy in android ad libraries*, Workshop on Mobile Security Technologies (MoST), 2012.

[5] Pearce P, Felt A P, Nunez G, et al. *Android: Privilege separation for applications and advertisers in android*, Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012: 71-72.

[6] China Anti-Virus alliance. *Specification for Mobile Internet Malicious Code*. Internet Society of China Network and Information Security Committee, 2011.