Trust It or Not? An Empirical Study of Rating Mechanism and Its Impact on Smartphone Malware Propagation

Wenjuan Li, Lijun Jiang, Weizhi Meng, Lam-For Kwok

Trust It or Not? An Empirical Study of Rating Mechanism and Its Impact on Smartphone Malware Propagation

Wenjuan Li[1], Lijun Jiang[1], Weizhi Meng[2]* and Lam-For Kwok[1]

[1] Department of Computer Science, City University of Hong Kong, Hong Kong
[2] Infocomm Security Department, Institute for Infocomm Research, Singapore
{wenjuan.li@my.cityu.edu.hk}

Abstract. Malicious applications (malware) have attracted much attention from both academia and industry. Thanks to this, common users start to install anti-malware tools to help protect their phones. However, we notice that attackers can still take advantage of some existing mechanisms to induce users to download malware and bypass anti-malware software. In this paper, we focus on the app rating mechanism on smartphones and aim to evaluate its impact on malware propagation. More specifically, we investigate how this mechanism can be maliciously used to leverage the trust levels of users and achieve particular goals (i.e., inducing users to download malware). In the evaluation, we develop a malicious rating system and conduct a study with over 400 participants. Our results indicate that such rating mechanism can affect users' trust on app download and can be utilized to propagate malware.

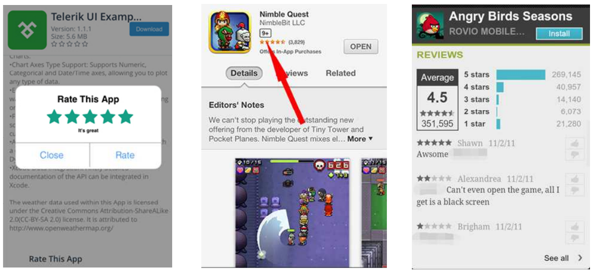
Keywords: Malicious Applications, Anti-Malware Software, Rating Mechanism, Smartphone Security, User Trust and Awareness.

1 Introduction

Thanks to the significant portability and the availability of mobile applications, smartphones have quickly become one prevalent computing platform. According to a report from the International Data Corporation (IDC), most existing markets will have a robust growth annually and the worldwide smartphone shipment volumes are forecast to reach 1.9 billion units by 2019 [2]. Since the popularity of smartphones increases, security challenges and threats also become a big concern on this platform.

Malicious applications (malware) are one of these challenges. There were more than 317 million new pieces of malware created in 2014, meaning nearly one million new threats were released into the wild each day [9]. Due to the large news reports and propaganda, more and more users are willing to install one kind of anti-malware software to safeguard their smartphones. In the literature, many efforts have been made through developing various advanced anti-malware

* The author was previously known as Yuxin Meng.



Charts.
•Chart Axes Type Support: Supports Numeric, Categorical and Date/Time axes, allowing you to plot any type of data.

documentation of the API can be integrated in Xcode.

The weather data used within this App is licensed under the Creative Commons Attribution-ShareALike 2.0(CC-BY-SA 2.0) license. It is attributed to http://www.openweathermap.org/

We can't stop playing the outstanding new offering from the developer of Tiny Tower and Pocket Planes. Nimble Quest mixes el... More ▾

Average		
4.5	5 stars	269,145
★★★★★	4 stars	40,957
351,595	3 stars	14,140
	2 stars	6,073
	1 star	21,280

★★★★★ Shawn 11/2/11
Awsome

★★☆☆☆ Alexandrea 11/2/11
Can't even open the game, all I get is a black screen

★☆☆☆☆ Brigham 11/2/11

(a) (b) (c)

Fig. 1. App rating mechanism: (a) rating action, (b) overall rating score and (c) rating score details and users' comments.

techniques. Differently, our interest in this work was motivated by the fact that attackers may invade users' phones through reducing user awareness, even if an anti-malware software is pre-installed.

In this work, we take *app rating mechanism* on phones as a case and conduct an empirical study to investigate its impact on users' trust and malware spread. In particular, we develop a *malicious rating mechanism* that can leverage the rating scores and comments of target apps. Our purpose is to investigate whether users can be induced to download those malicious apps under the rating system. If users download and install these apps, a self-defined message will be sent to our server and a high rating score will automatically give to those apps in turn. Totally, over 400 users are involved in our study and provide their feedback about their attitude and behaviors. The study results are evaluated based on statistical data and users' feedback. To sum up, the results reveal that attackers can make use of rating mechanisms to reduce user awareness and increase their trust levels on app download, which may greatly degrade the effectiveness of anti-malware tools and cause malware propagation on smartphones.

The remainder of this paper is organized as follows. Section 2 introduces the typical rating mechanism and Section 3 describes the developed malicious rating system that was used in the study. Then, Section 4 illustrates our study methodologies and analyzes the collected results, and Section 5 discusses related studies. Finally, we conclude our work in Section 6.

2 Rating Mechanism

This rating mechanism is a user feedback channel, attempting to encourage users to share their experience for downloaded apps. The major purpose of this mechanism is to promote the high rating apps and to allow users to share their experience associated with their used apps. Several examples of this mechanism are depicted in Figure 1. Specifically, Figure 1 (a) shows the rating action (i.e., giving a rating score to an app), Figure 1 (b) describes the overall rating score for an app and Figure 1 (c) presents the rating score and users' comments. To summarize, there are three main features of a typical rating mechanism: 1) the rating score usually ranges from 1 to 5, where 5 indicates the highest score (satisfied); 2) the overall rating score is shown on the downloading page of an app and 3) for each app, the details of rating score (e.g., votes for each score) and users' comments are available to all users.

3 Malicious Rating System

As the app rating mechanism may play an important role in users' downloading choice, it is possible for attackers to utilize it to reduce user awareness and increase their trust on particular apps. To validate this, we develop a malicious rating system and its high-level architecture is depicted in Figure 2. In real-world cases, this alternative market can be popular under some scenarios. For example, an app is not free in official markets but is available in an alternative market (e.g., Anzhi market [1]).

3.1 Popular App Category

To simulate a typical app market, it is expected to provide more popular apps that are likely to be downloaded by users. To achieve this goal, we conduct a survey about popular app categories with 729 participants. The concrete question is: *what is your most frequently downloaded app category.* Each participant can only vote one category. The voting results are shown in Figure 3.

It is found that up to 302 participants (with a rate of 41.4%) are frequently to download *entertainment apps* (e.g., games). There are 183 participants (about 25.1%) are often to download *tool apps.* In contrast, few participants (less than 2%) download *puzzle* and *education apps* in their spare time. Based on these results, we deploy apps in the market with a similar distribution (i.e., entertainment apps are the most).

3.2 Market Settings and Malicious Rating

In this section, we discuss how to construct the app market in detail and how the malicious rating system works.

- **Market construction.** According to the app distribution in Figure 3, our app market is configured to contain a total of 1405 apps, where 603 of them are entertainment apps, 354 of them are tool apps and the remaining apps belong to other relevant categories. Users can connect to the market through a web link, search and download apps to their mobile phones. The rating scores (the highest score is 5) and users' comments would be shown on each app-downloading page.
- **Malicious rating system.** To deploy those malware to our market, we camouflage 500 entertainment and 300 tool apps using such malware. Moreover, to explore the effect of rating scores on users' choice, 300 entertainment apps were given a high rating score between 4.5 and 5, while the other entertainment apps were given a low rating score between 2 and 2.5. It is the

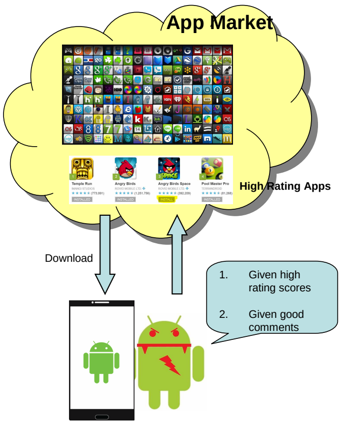


Fig. 2. The high-level architecture of our malicious rating system.

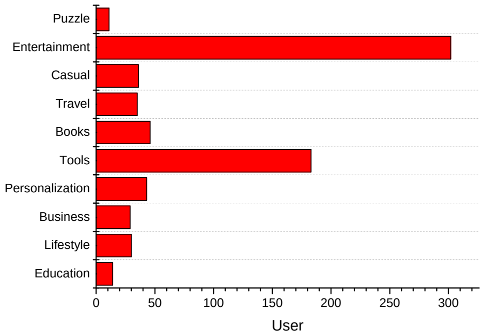


Fig. 3. A survey of popular app category.

same for other app categories, in which only half of them were given a high score. After users' installation of our malicious apps, a message will be sent to the server. Afterwards, the server will give the highest score (5 score) to that app and generate a corresponding benign comment.

4 Our study

Due to security reasons, it is not feasible to use an existing app market in our study directly. In this case, we developed a web-based app market (named as *Popstar market*) on our self-maintained server, in which its structure and workflow are similar to the existing Anzhi market [1].

4.1 Study Methodology

In the study, most participants were recruited from a university environment, since students are one of the main body of smartphone users. Before the study, we got approvals from the university and security office, so that we can use an online system to recruit participants. All study deployment and processing were not relevant to the university environment. More specifically, we mainly conducted two case studies: *in-lab study* and *out-lab study*.

- **In-lab study.** Participants were recruited online, where a total of 317 students were willing to attend this study. None of them were from security-related majors. All participants were invited to our lab and were given an Android phone. The phone was pre-installed an antivirus tool that can make an alert when the user encounters and installs the developed malware. This

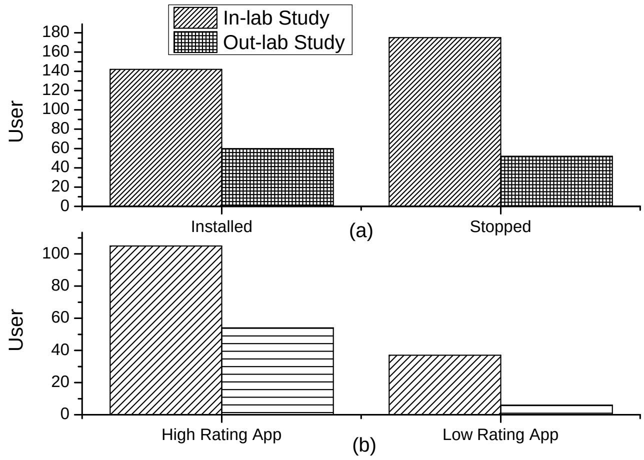


Fig. 4. (a) Infection rates for in-lab and out-lab conditions, and (b) Installed high rating apps versus low rating apps.

design aims to explore whether users will ignore such kind of alerts. In addition, before the study, we explained our goal to all participants, and they were required to download up to 15 apps. After the study, all participants were given a questionnaire form to provide their feedback. A gift card $10 will be given to each participant as incentive.

- **Out-lab study.** In order to simulate a real scenario, we conducted another case study, where users did not need to come to the lab environment to complete their tasks. In fact, all participants should use their own phones to finish the study. For this purpose, 112 new students were recruited online. None of them were from security-related majors. Before the study, we introduced our objectives to all participants. Similar to our tasks in the in-lab condition, all participants were asked to download 15 apps from our market. After the study, all participants were invited to give feedback on a questionnaire form. Finally, 109 participants were consent to give feedback and approved us to use the statistical data. In this case, we only analyze the data from these 109 participants and all of them were given a $10 gift card as incentive. The whole study took three weeks to finish.

4.2 Statistical Results

According to our system design, as long as one participant successfully installed the malicious app, our server can receive a message for that app. This can help compute statistics relevant to users' choice and actions during the app download. After the study, we calculate the statistical results based on the received messages from the server. The infection rates and the numbers of installed high and low rating apps are shown in Figure 4.

Table 1. User feedback during the study.

Questions/users	*In-lab*	*Out-lab*
Q1. I prefer to download my interested apps	188	96
Q2. I prefer to download high rating apps	226	100
Q3. Did you check others' comments before downloading	242	99
Q4. Did you notice any app requiring to disable antivirus software	270	97
Q5. Did you stop any antivirus software before downloading apps	142	60
Q6. Were you aware of any risk of downloading apps in the market	171	55

- **In-lab study.** Figure 4 (a) shows that up to 142 participants suffered from the malicious rating system and installed the malware, in which the infected rate is 44.8%. In the study, it is observed that those infected participants have ignored the pop-up alert and disabled the pre-installed anti-malware software. To look closer to the installed number of different rating apps, Figure 4 (b) shows that those participants are very likely to continue installing an application with a high rating score, instead of installing a low rating app. The figure presents that nearly 74% installed malicious applications are high rating apps, while only 26% apps with low rating scores.
- **Out-lab study.** The main purpose of this study is to investigate users' behavior in a practical environment. Under the out-lab condition, users can use their own phones to search and download apps from our market. Similarly, the infection rate and installed app numbers are shown in Figure 4. Figure 4 (a) shows that up to 60 participants continued installing the malicious apps on their own phones so that the infected rate is 53.6%. The infection rate is a bit higher than that of the in-lab study. According to Figure 4 (b), participants were mostly willing to continue the installation of high-rating apps, where 90% successful cases came from high-rating apps.

4.3 User Feedback

In this part, we analyze the collected user feedback regarding their choice, awareness and trust levels during the app download. Some key questions and user feedback from both case studies are summarized in Table 1.

App download choice. In Table 1, the first question reflects that 59.3% participants selected to download high-rating apps in the lab environment, but more than 85% participants did so outside the lab (in the second user study). In contrast, in the out-lab study (with their own phones), users prefer to start downloading their interested apps. The numbers of this question indicate that users usually begin downloading an app according to their interests, even under a constrained condition.

In Table 1, the second question shows that 226 out of 317 participants (about 71.3%) were likely to download high-rating apps under the in-lab condition, while 100 out of 109 participants (about 91.7%) prefer to download high-rating apps under the out-lab condition. The latter is much higher than the former due to environmental factors, whereas both rates verify that users are willing to install high-rating apps. They generally believe that high-rating apps are more secure than those low rating ones. For example, if there are several app versions, they are more likely to download the version that has a higher score.

User trust. The third question shows that up to 76.3% and 90.8% participants in respective condition will check others' comments before they download an app. In our interview, it is found that users' comments have a high impact if the app download or installation encounters some issues. For example, when the app installation is alerted by an antivirus, users will check others comments to confirm the situation. If the comments are good enough, users may decide to ignore the alert and continue the installation.

Regarding the fourth question, most participants (over 85%) notice that some apps require to disable anti-malware software before downloading & installing the apps. The fifth question shows that nearly half participants would follow the instructions to disable the anti-malware software and continue the installation. In our interview, most infected participants considered that this may be a common case for some entertainment and tool apps, especially in a new market, that false alarms often occur.

User awareness. The last question shows that only about half participants (53.9% and 50.4% for each condition) are really aware of any risk in downloading apps from our market. Most participants considered that those apps, especially high-rating apps, should be benign and at least not harmful, since the rating scores and comments are quite good from others.

Discussions. Overall, based on the feedback, it is validated that rating scores and comments can greatly affect users' trust on app download. That is, the rating mechanism can impact users' attitude in downloading an app from a market. Therefore, through proper camouflage, attackers can utilize such rating mechanism to induce users to disable anti-malware tools and continue downloading & installing particular apps. This situation opens a hole for attackers to spread malware even if users have pre-installed antivirus software.

5 Related Work

As smartphones have become a major target for attackers, various research studies have focused on the detection of malware from market [8, 10]. There are also some studies discussing recommender and rating systems [3, 7]. Different from those studies, in this work, we target on app rating mechanism and attempt to evaluate its impact on users' trust on app download and malware propagation on smartphones. From this aspect, to the best of our knowledge, our work is the first study in the literature to investigate this topic.

Our study reveals that users' trust can be greatly affected by a malicious rating system and be induced to download malicious apps, resulting in malware propagation. Even worse, it is worth noting that such malicious rating system can collaborate with existing advanced malware techniques to achieve an even larger impact (i.e., stealing users' sensitive information and data). There is a line of research studies on applying various attacks to infer users' private information and data on smartphones, including side channel attacks [5] and physical access attacks like charging attacks [4, 6].

6 Conclusion

Different from other studies on rating systems, in this paper, we focus on app rating mechanism on smartphones and aim to evaluate its impact on users' trust and malware propagation. We have two specific questions: whether users can be induced to download malicious apps, and whether the rating systems can affect users' trust on app download. Our results indicate that users' trust can be greatly affected by such system by manipulating high rating scores and good comments. By taking advantage of this system, attackers can propagate malware and bypass antivirus tools. Our research attempts to raise more attention for malware research community on user-centric solutions.

References

1. Anzhi Market. www.anzhi.com/.
2. Global Smartphone Growth Expected to Slow to 11.3% in 2015. (Accessed on June, 2015): http://www.idc.com/getdoc.jsp?containerId=prUS25641615.
3. Josang, A: Robustness of trust and reputation systems: Does it matter? In: Proceedings of the 6th IFIPTM, pp. 253-262 (2012)
4. Meng, W., Lee, W.H., Murali, S.R., Krishnan, S.P.T.: Charging Me and I Know Your Secrets! Towards Juice Filming Attacks on Smartphones. In: Proceedings of ACM CPSS, pp. 89–98 (2015)
5. Meng, W., Wong, D.S., Furnell, S., Zhou, J.: Surveying the Development of Biometric User Authentication on Mobile Phones. IEEE Communications Surveys & Tutorials 17(3), pp. 1268–1293 (2015)
6. Meng, W., Lee, W.H., Krishnan, S.P.T.: A Framework for Large-Scale Collection of Information from Smartphone Users based on Juice Filming Attacks. The Singapore Cyber Security R&D Conference (SG-CRC), pp. 99–106 (2016)
7. Muller, T., Liu, Y., Mauw, S., Zhang, J.: On Robustness of Trust Systems, In: Proceedings of the 8th IFIPTM, pp. 44-60 (2014)
8. Peng, S., Yu, S., Yang, A.: Smartphone malware and its propagation modeling: A survey. IEEE Communications Surveys and Tutorials 16(2), pp. 925–941 (2014)
9. Symantec. Internet Security Threat Report, Volume 20, 2015. (Accessed on June, 2015): http://www.symantec.com/security_response/publications/threatreport.jsp.
10. Teufl, P., Ferk, M., Fitzek, A., Hein, D., Kraxberger, S., Orthacker, C.: Malware detection by applying knowledge discovery processes to application metadata on the Android Market (Google Play). Security and Communication Networks 9(5), pp. 389-419 (2016)