ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (1-3), Month: July - September 2016, Available at: www.researchpublish.com

Pre-emptive Risk Determination for Improved User Experience in Android Applications

Sushil Kumar[1], Akhilesh Yadav[2], Ramesh Solanki[3], Vaishali Gatty[4]

[1]PG Scholar, Dept of MCA, VES Institute of Technology, Mumbai, India.
[2]PG Scholar, Dept of MCA, VES Institute of Technology, Mumbai, India.
[3]Assistant Professor, Dept of MCA, VES Institute of Technology, Mumbai, India.
[4]Assistant Professor, Dept of MCA, VES Institute of Technology, Mumbai, India.

Abstract: **This research paper is carried out on mobile apps and their security issues. Most of the users don't know the risk involved in sharing their personal data with the apps. This research will make awareness in users about risk involved in sharing their personal data and then see the effect of awareness in the users while installing the app.**

Keywords: **Android Applications, Personal Data.**

1. INTRODUCTION

The world has very quickly evolved into a mobile technology driven civilization over the past decade. Research carried out previously shows that only 19% of Android users are consciously aware of specific app installation permissions [1]. User awareness regarding leakage of private information is low thereby resulting in ambiguity and complications. Kelly et al. introduced a modified app information screen which resulted in reduced installs of apps requesting too much permission. Kelley et al. argues that potential risks arising from excessive app privileges are not part of user's decision process because permissions are shown only after the installation button has been pressed [3]. While they increased awareness of requested permissions, users were still unsure about threats arising from these apps.

Users show limited awareness of threats and risks to their personal data during the selection and installation of a new app. Our approach to this issue emphasizes on sensitizing the user about these problems at the outset. Hettig et al. [5] came up with a novel approach wherein they illustrate risks arising from app permissions by providing worst-case examples that demonstrate potential attack scenarios resulting from the malicious use of the requested permissions. Rader et al. [4] proved the importance of peer group awareness regarding applications by showing that many users learn about security from informal stories told by family and friends.

This paper deals with a novel approach wherein we improve user awareness regarding how applications behave in order to improve risk assessment surrounding app permissions. Our test study evaluates the effectiveness of this approach. App installation counts of the original Android market with our improved display are compared.

2. METHOD

A large number of rarely used permissions are defined by the Android OS [2]. Eight permissions commonly used by popular apps are chosen as reference. The most common permissions are chosen by considering the research carried out by Hettig et al. wherein they crawled 17,888 most popular apps on the Android Play Store in early 2016 [5].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (1-3), Month: July - September 2016, Available at: www.researchpublish.com

Table 1: Permissions selected for evaluation and percentage of app requests [5].

Permission	Requests (%)
full network access	75%
modify external storage	52%
read phone status and identity	39%
precise location	29%
use accounts on the device	27%
take pictures and videos	25%
read contacts	12%
read call log	5%

A mock up study was carried out on the Play Store[2]. Conventional representation of permissions was accompanied by a threat perception graph with a vivid graphical representation. We presented a concise statistical analysis how each permission can affect user data or phone performance prior to app installation. This presented the user with projected worst case scenarios and also the effect on device performance and consequences with respect to user data.

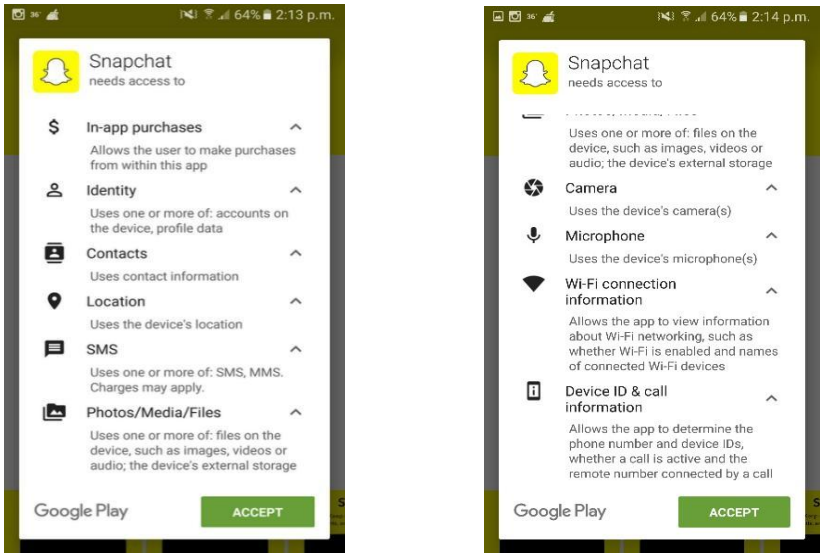

Figure 1: android permissions prior to installation of 'Snap chat' Android application

A larger sample size helped us understand user response better. Four different app categories with eight apps per category were used. The following permissions were requested:

- Office apps permissions (network, phone status and identity, modify external storage)
- Finance apps permissions (Permissions including camera, location)
- Weather apps permissions (Permissions including modify external storage, camera)
- Games apps required no permissions at all.

We note that apps within the same category generally asked for a similar set of permission. Permissions were varied perhaps to judge the precise impact on user installation decision.

Participants or volunteers were invited first within a closed group and then randomly. General behavior of the user during app installation and concerns were judged with request response mechanisms built into our testing approach. After obtaining consent, our test app was installed in participant's devices to create information overlays during app installations. This improved user awareness regarding the impact of various app permissions and their response was studied. For better understanding, a set of users was also asked to install the apps normally without our test app. This enabled us to understand the impact our approach had on users based on how many were influenced to change their decisions based on our information overlay screens. A final debrief and question and answer session was held to clarify our understanding.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (1-3), Month: July - September 2016, Available at: www.researchpublish.com

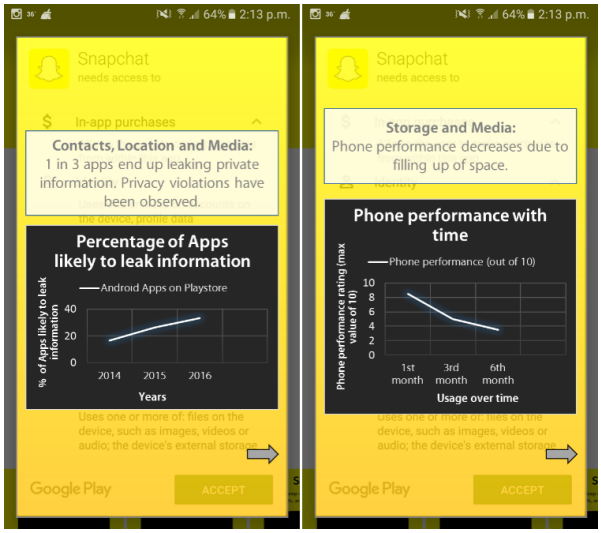

Figure 2: Sample information overlay screens provided by test app prior to app installations from android play store.

3. STUDY RESULTS

32 participants (inclusive of 12 women, 10 participants with computer science background and 8 non-technical backgrounds) people were considered. Direct app installswithout our test app showed that participants installed 4.2 apps on average. However, when the test app was used, participants only installed 3.1apps.This clearly supports the observation that better threat perception influenced peoples' decision regarding which apps to install. There was also a drastic reduction in app installations of apps in specific categories like finance and weather where irrelevant and excessive permissions were required. This installation figure dropped to below 10% of total apps. The response of the participants to better awareness regarding threats and security issues was very encouraging. Clear differentiation was obtained regarding user interaction with apps based on better awareness and risk perception. 60% of participants indicated their concerns regarding privacy and security of personal information while installing an application. Further, 80% of participantsindicated greater awareness and care while installing new applications in the future.

4. CONCLUSION AND FUTURE WORK

This paper demonstrates the positive impact of relevant and guided information exchange with the user to help him avoid security risks that may arise while using android applications. A novel approach which provides statistical data overlays regarding risk factors was proposed and positive user reception to the idea was observed. Users based their android application installation decisions on concrete data thereby increasing comfort and realizing more secure ways of using these applications.

Future work entails extension of our study to a wider group of people and better variety in type of applications. Further, we would like to study the impact of exact app specific information over a period of time on people. Successful completion of the study would provide scope for utility in network security and user awareness, improving user experience and streamlining security guidelines for app development in the market. Dynamic updates regarding security hazards and potential flaws can be studied which will benefit the user in safeguarding his or her private information better.

REFERENCES

[1] P. Felt, E. Chin, S. Hanna, and D. Wagner. Android permissions demystified. In Proc. CCS. ACM, 2011.

[2] P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android Permissions: User Attention, Comprehension, and Behavior. In Proc. SOUPS. ACM, 2012.

[3] P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy asPart of the App Decision-Making Process. In Proc. CHI.ACM, 2013.

[4] E. Rader, R. Wash, and B. Brooks. Stories as InformalLessons about Security. In Proc. SOUPS. ACM, 2012.

[5] M. Hettig, E. Kiss, J.-F. Kassel, S. Weber, M. Harbach, M. Smith. Visualizing Risk by Example: Demonstrating Threats Arising From Android Apps. In Proc. SOUPS.2013, UK.