Usability Study of a Mobile Privacy Application

Clare Lai
Jianlan Zhu
Sharada Boda
Ting Lu
Carnegie Mellon University
Pittsburgh, Pennsylvania
cxlai@andrew.cmu.edu
jianlanz@andrew.cmu.edu
sboda@andrew.cmu.edu
tilu@andrew.cmu.edu

Abstract
Usability is rapidly becoming a major concern for software developers due to increasing ubiquity of technology. Redmorph Inc. is a privacy and security company developing applications for the average user [6]. In this study we conducted a diary study to examine the usability of the Redmorph mobile application for Android. Since the application is advertised as easy to use, the user study compared metrics of learnability and user satisfaction over the course of a week when using the app. Our research will focus on whether the user can understand the technical jargon in Redmorph, whether they can configure the app, how well they can use various features and in which scenarios Redmorph breaks the functionality of existing apps. Our results suggest that even the 'average' user base includes many different levels of technological expertise. We provide various recommendations to improve the usability which hold true for other security apps.

Author Keywords
Privacy, Security, Mobile app, Usability Study

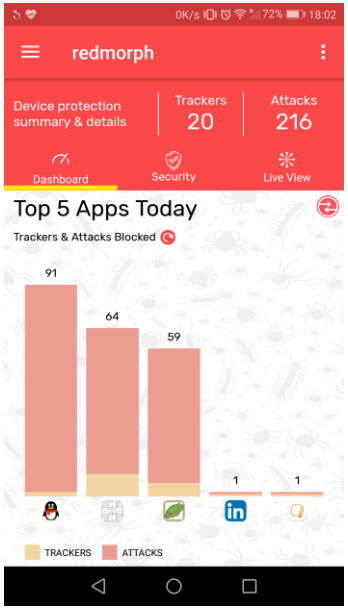

Figure 1: Dashboard Page

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous; See http://acm.org/about/class/1998 for the full list of ACM classifiers.

Motivation and Related Work

The goal of our study is to study the usability of a mobile app, which is developed by Redmorph to protect user's privacy and security from online tracking on their Android phone. Our study of the Redmorph mobile application attempts to gauge user attitudes and understanding during regular usage of the app.

The third-party eco system on mobile phones tracks and collects user information based on app permissions [2,5]. The research community has used various methods towards understanding this ecosystem [5]. Vallina-Rodriguez et. al. built an app to analyze network traffic [5]. The results showed that 63% of the domains in the network belonged to the advertisement and tracking services [5].

Adoption of Ad-blocking mechanisms has become a widespread practice [7]. As of March 2016, 300 million users were blocking ads on their smartphones [7]. Garimella et. al analyzed the performance of Ad-blockers in browsers on mobile and desktop devices [3]. The research aimed to understand the effectiveness of Ad-blockers in protecting the user from tracking mechanisms by analyzing network traffic and performance related factors such as change in loading time, number of threads and background processes [3]. Ikram and Kaafar performed static analysis on Ad-blocking apps [4]. It was determined that at least 68% of Ad blockers have third-party trackers embedded into their code and 89% of Ad-blockers request access to sensitive information [1].

Although much research has been done to analyze the performance of various Ad-blocking and tracker blocking tools in the mobile ecosystem and many usability studies have been conducted in the security and privacy domain, we believe that this is the first usability study on an Ad-blocking app in the mobile ecosystem so far.

Methodology

The study had four parts beginning with a pre-screening survey distributed to the Carnegie Mellon University Center for Behavioral and Decision participation pool. A pre-interview was conducted to gauge user attitudes before a week-long diary study, during which users recorded responses and behaviors online. The study concluded with a post-interview. Analysis focused on qualitative data from the interviews and diary entries. The qualitative data was coded to determine the participants' perceptions and attitudes on using the app.

The study was conducted with a total of 13 participants. 7 of the participants were female, and 6 were male. 7 participants had some computer course experience and 6 did not. Participants' ages range from 18 to 60. The number of apps on their phones are equally distributed as well.

The study focused on the participants experience during app installation and on the three main screens in the app - dashboard page, security setting page and live view page (Figure 1, Figure 2 and Figure 4). The dashboard page (Figure 1) provides a summary of the

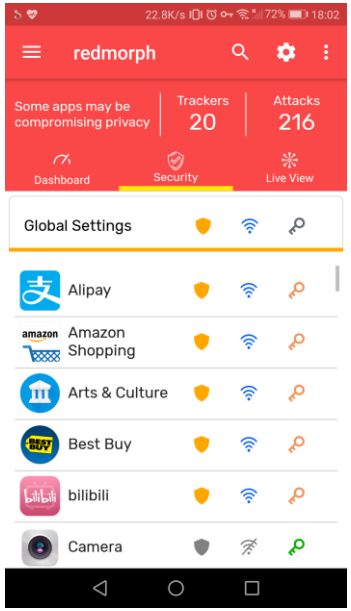

Figure 2: Security Page

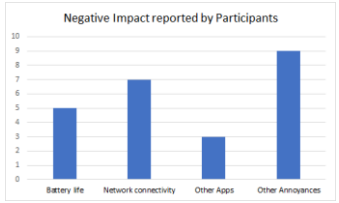

Figure 3: Negative Impact reported by Participants because of Redmorph

trackers and blockers. The security page (Figure 2) allows the users to configure and assess other apps on their phone with the help of three primary icons - the shield, the Wi-Fi icon and the key. The live view (Figure 4) provided the a graphical and a list view of all the trackers and showed the connections with the apps.

Results and Discussion

Overall, the users were satisfied with the app. They found the app useful, easy to use and usable. However, they were quite unwilling to recommend the app as they felt that they themselves did not understand the app.

Participants' Understanding of Technical Jargon

Redmorph uses VPN (Virtual Private Network) to monitor tracking. The Android operating system provides a confirmatory popup before allowing Redmorph to setup the VPN. Before this popup is shown, Redmorph provides a custom popup with an explanation for the VPN. However, this popup is labelled as 'Congratulations' and more than half the participants swatted the popup away. Therefore, most participants were surprised when they saw the Android operating system ask for confirmation regarding VPN permission. The participants who weren't familiar with VPN were concerned and worried about the implications of installing the app.

The Redmorph application use revolves around the concept of trackers. Therefore, we assessed the participants' understanding of what trackers are during the pre-interview and post-interview. There were overall four different categories of perspectives on what trackers are. The participants either had no knowledge, associated all trackers with collecting physical location, had a general broad understanding of what trackers are, or considered all trackers as malicious. One of two participants who had no knowledge of trackers before using the app, developed a more comprehensive understanding. However, two of the participants who had a more comprehensive understanding, began looking at most trackers as malicious after using the app for a week.

Retention of Information

During app installation, Redmorph provided an overlay form which explained the various features in the app. The overlay form is a transparent page which provides a step-by-step tutorial. Though all the participants looked at the overlay form, none of the participants could accurately remember all the explanations. Few participants felt that there was an overload of information. One participant mentioned that he wants more information in minimal text. The participants were mostly looking for small help icons that they could click to get more information as and when required.

Effect of Usability Issues

The participants experienced a range of issues during app usage which included reduced battery life, reduced internet speed or performance issues in other apps (Figure 3). Only 2 participants did not report any issues. Despite the difficulties, 11 out of 13 participants them felt that Redmorph was too useful to uninstall. One participant mentioned that she would reduce the screen brightness to compensate for the resources that Redmorph was consuming.

Participants' Perception of Safety after Using the App

The participants were asked whether they felt safer after installing the app in the pre-interview and the

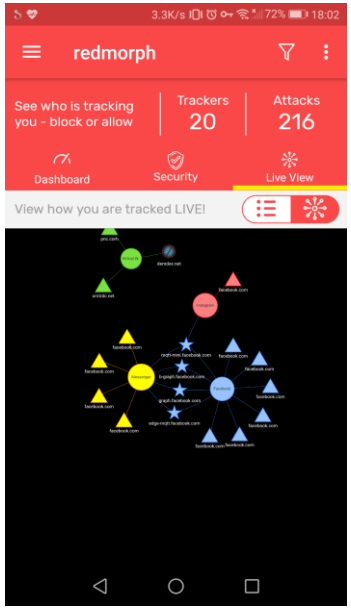

Figure 4: Live View

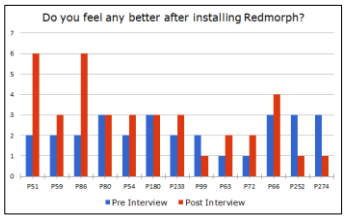

Figure 5: Do you feel any better after installing the app

post-interview (Figure 5). They were asked to rate on a 7-point Likert scale where 1 was "very safe" and 7 was "not safe at all. Four participants showed at least a 2 point difference between their pre-interview responses and post-interview responses. Two of the participants rated that they were more concerned after using Redmorph and two participants rated that they were less concerned. Among the two participants who mentioned that they were more concerned, one participant did not find Redmorph useful but was concerned about the tracking taking place. The other participant was quite confused with the app and wasn't sure what to do and therefore, felt more concerned. The participants who expressed that they were less concerned mentioned that they felt better because they installed Redmorph.

An interesting data point was why the participants felt safe after using Redmorph. While one common reason was that Redmorph was acting as a firewall, another common reason was that they were pro-actively able to do something. When the participants mentioned proactiveness, they did not merely refer to installing Redmorph and setting it up. Rather, the participants felt that by disabling the network or enabling protections on other apps using Redmorph, they were proactively taking actions to improve their personal security.

Categories of Users

From the existing data, we found that there were two categories of user. One set of users wanted an app that would take at most 10 minutes to set up and run in background without any issues. Another set of users wanted to proactively configure each app. However, all the users wanted more information which included explanation of technical jargon or more information on trackers to help them decide how to protect themselves better.

General Recommendations

In general, our recommendations would be to provide all explanations in appropriate popups. It would also be better to reduce the content on overlay form and instead provide information through help icons. Additionally, we would recommend the reduction of technical jargon or more explanation of these terms. We also recommend clearly distinguishing between similar features specifically, the key and the shield. Configurable and non-configurable items should also be separated. The settings shown by clicking the key icon was not configurable. However, the settings shown by the shield and Wi-Fi icon were configurable. The participants were confused as to what each represented. For development of other security applications aimed at consumers without specialized technical knowledge, these recommendations also hold. Information necessary to understanding the app should be provided to all users. With the additional information, users will likely be able to make better use of the functions of the application and experience a better level of usability and effectiveness.

Acknowledgements

We thank Professor Lorrie Faith Cranor for her guidance on the project, teaching assistant Javed Ramjohn for his assistance, and all of the participants and Redmorph for their cooperation.

References

[1] Carolyn Brodie, Clare-Marie Karat, John Karat and Jinjuan Feng. 2005. Usable security and privacy: a

case study of developing privacy management tools. In Proceedings of the 2005 symposium on Usable privacy and security - SOUPS '05. ACM Press, New York, NY, 35-43. DOI:https://0.1145/1073001.1073005

[2] Diana. K. Smetters and Rebecca. E. Grinter. 2002. Moving from the Design of Usable Security Technologies. In Proceedings of the 2002 workshop on New security paradigms (NSPW '02). ACM Press, New York, NY, 82-89. DOI:https://doi.org/10.1145/844102.844117

[3] Kiran Garimella, Orestis Kostakis, and Michael Mathioudakis. 2017. Ad-blocking A Study on Performance, Privacy and Counter-measures. In Proceedings of the 2017 ACM on Web Science Conference - WebSci '17 (2017). ACM, New York, NY, USA, 259-262. DOI: https://doi.org/10.1145/3091478.3091514

[4] Muhammad Ikram and Mohamed Ali Kaafar. 2017. A first look at mobile Ad-Blocking apps. 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA) (2017). Cambridge, MA, 2017, pp. 1-8. DOI: http://dx.doi.org/10.1109/nca.2017.8171376

[5] Narseo Vallina-Rodriguez, Srikanth Sundaresan, Abbas Razaghpanah, Rishab Nithyanand, Mark Allman, Christian Kreibich and Phillipa Gill. 2016. Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem. Retrieved from https://arxiv.org/abs/1609.07190

[6] Redmorph INC. Retrieved from https://redmorph.com/help.html

[7] The PageFair Team. 2017. 2016 Mobile Adblocking Report. (July 2017). Retrieved from https://pagefair.com/blog/2016/mobile-adblocking-report/