Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Delegate the smartphone user? Security awareness in smartphone platforms

*Alexios Mylonas, Anastasia Kastania, Dimitris Gritzalis**

Information Security and Critical Infrastructure Protection Research Laboratory, Department of Informatics, Athens University of Economics and Business (AUEB), 76 Patission Ave., Athens GR-10434, Greece

ARTICLE INFO

Article history:
Received 14 April 2012
Received in revised form
4 October 2012
Accepted 20 November 2012

Keywords:
Application markets
Security awareness
Security survey
Smartphone platforms
Smartphone security

ABSTRACT

Smartphone users increasingly download and install third-party applications from official application repositories. Attackers may use this centralized application delivery architecture as a security and privacy attack vector. This risk increases since application vetting mechanisms are often not in place and the user is delegated to authorize which functionality and protected resources are accessible by third-party applications. In this paper, we mount a survey to explore the security awareness of smartphone users who download applications from official application repositories (e.g. Google Play, Apple's App Store, etc.). The survey findings suggest a security complacency, as the majority of users trust the app repository, security controls are not enabled or not added, and users disregard security during application selection and installation. As a response to this security complacency we built a prediction model to identify users who trust the app repository. The model is assessed, evaluated and proved to be statistically significant and efficient.

1. Introduction

Unlike PC software, smartphone applications (or 'apps') adopt centralized distribution architectures and are usually available to users from app repositories or app marketplaces. These app repositories may either be official (i.e. maintained by the smartphone platform, e.g. Apple's App Store, Microsoft's App Hub), or not (e.g. Amazon Appstore for Android). The security models of smartphone platforms provide different options with respect to the permitted source of applications (Barrera and Van Oorschot, 2011; Mylonas et al., 2011a). In addition, the strictness of app vetting controls in an app repository[1] ranges from relaxed app submission in community-based app repositories, such as Google play, to strictly controlled repositories that follow the 'walled garden' model, such as Apple's App Store (Barrera and Van Oorschot, 2011; Mylonas et al., 2011a, 2011b). Regardless of how strict and centralized the security model of a platform may be, it always leaves some choice to the user. Again, this delegation can be simply authorizing access to some protected resources, or may give user the choice to infer if an application may impair her security and privacy.

Meanwhile, the rate of downloads for smartphone applications from app repositories is on the rise (Baghdassarian and Milanesi, 2010). This popularity of smartphone applications has drawn the attention of attackers, who try to use the app repository as a security and privacy attack vector. In this context, an increasing number of malicious applications have already been discovered in app repositories (Felt et al., 2011b; Zhou et al., 2012b).

This is one of the reasons that smartphones have also drawn the security literature's attention. The security literature that focuses on smartphone applications has elaborated on malicious application identification (Egele et al., 2011; Enck

* *Corresponding author*. Tel.: +30 2108203505; fax: +30 2105810116.
E-mail addresses: amylonas@aueb.gr (A. Mylonas), ank@aueb.gr (A. Kastania), dgrit@aueb.gr (D. Gritzalis).

[1] Unless stated otherwise, in the rest of the paper the term "app repository" refers to an official app repository.

0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.11.004

et al., 2009,2010, 2011; Nauman et al., 2010; Zhou et al., 2012a, 2012b; Zhou and Jiang, 2012). Automated scanners have been proposed to aid advanced users deduce whether an application requests permissions that can impair the security and\or privacy of users (Enck et al., 2010; Felt et al., 2011a; Hornyack et al., 2011). Nonetheless, it is unclear whether the burden of making security decisions is reasonable for normal users. Studies have shown that normal users are not able to make such decisions, nor are able to use security controls adequately (Furnell, 2005, 2007; Furnell et al., 2006; Whitten and Tygar, 1999).

In this paper, we examine the security awareness of smartphone users who install applications from official app repositories. We conducted a survey with the aim to answer the following main research questions:

Q1: Do smartphone users enable security controls on their devices?
Q2: Do users consider security while choosing and downloading applications?
Q3: Do smartphone users trust applications from the official app repository?

The survey scope includes only users who download applications from the official app repositories of the current popular smartphone platforms, i.e. Android, BlackBerry, iOS, Symbian and Windows Phone. Our survey results indicate a clear lack of smartphone users' security awareness. Contrarily to Q1 and Q2, the security unaware users of Q3 cannot be identified with the use of software, e.g. smartphone agents, Mobile Device Management (MDM) (Redman et al., 2011), etc. For this reason, we propose and evaluate the effectiveness of a prediction model that identifies users who trust applications from the app repository.

The rest of the paper is organized as follows. The next section presents related work. Section 3 provides the reader with the methodology of the survey. In Sections 4 and 5 the findings from the summary of the sample responses and the essential statistical analysis are presented, respectively. In Section 6 the prediction model is described and its effectiveness is evaluated. Finally, Section 7 includes the survey's limitations, whereas Section 8 includes a discussion of the results and conclusions.

2. Related work

Even thought smartphones are well studied in security literature, the relevant research work on the security awareness of smartphone users is currently rather limited and mainly focuses on Android. Chia et al. (2012) studied risk signalling concerning the privacy intrusiveness of Android applications in two application repositories, i.e. Android market[2] and AppBrain.com. Their results suggest that the number of dangerous permissions that an application requests is positively correlated with its popularity. Even though users understand the notion of application popularity, the fact that an application is popular does not imply that it respects the users' privacy. Moreover, their results indicate that the current risk signals employed by an app repository (e.g. developer's website, application reputation) become ineffective over time, as users tend to click through them. Our findings also indicate that users tend to ignore the reputation and the reviews of an application, as well as the security and agreement messages revealed during application installation from app repositories.

Similarly to our user survey, smartphone users were found to ignore security messages during application installation in (Felt et al., 2012; Kelley et al., 2012). Moreover, they were unable to comprehend the permissions and the risks that are related with them (Felt et al., 2012; Kelley et al., 2012). As a result, in both studies the Android security messages did not assist most users to make appropriate security decisions. Our results suggest that the majority of respondents ignore every aspect of security and privacy during application selection, as well as the app's reputation, reviews and security and agreement messages. Nonetheless, when explicitly asked, a minority of users in the survey conducted by Felt et al. (2012) reported that they have cancelled the installation of an application due to its permission requests. In our survey a minority of users was found to delve into security and agreement messages; they tend to be security and technology savvy.

Finally, in the user study conducted in (Kelley et al., 2012) users erroneously believed that applications undergo security analysis during their submission in the Android Market. In our study we also found such misconceptions about application testing in application markets. Moreover, most users were unaware of the existence of the application testing mechanism.

3. Methodology

To assess the security awareness of smartphone users, a survey was conducted from September to December 2011, in Athens, Greece. This section presents the survey methodology, as well as some details about the tests mounted so as to ensure the validity and statistical significance of the results.

3.1. *Data collection*

The survey responses were collected from random people on the street and from public transport means (train stations, underground, airports), via structured interviews (Flick, 1998). A questionnaire (see Appendix B) was used for the structured interviews. The duration of the interview completion was 5–8 min, on average. The discussion with the user aimed to ensure the validity of her responses, the comprehension of the questions, and the comprehension of technical terms.

Questions 5 and 7 were used to filter out the non-smartphone users and the smartphone users who did not install third-party applications in their devices. We excluded these two user groups because the survey focused on smartphone users who do download applications from app repositories. Questions 2 and 8 were the only free text questions.

[2] Android Market is the smartphone app repository Google maintained before merging and rebranding it with other digital content services in Google Play (http://googleblog.blogspot.com/2012/03/introducing-google-play-all-your.html, March 2012).