Mobile Applications Security: 
Role of Privacy

Emergent Research Forum (ERF)

Hamid Reza Nikkhah  
University of Arkansas  
Hnikkhah@walton.uark.edu

Ali Balapour  
University of Arkansas  
ABalapour@walton.uark.edu

Rajiv Sabherwal  
University of Arkansas  
RSabherwal@walton.uark.edu

Abstract

Mobile users still express their concerns about security of mobile applications because these applications have access to personal information stored on mobile devices. Mobile applications developers constantly provide new solutions to enhance security of mobile applications, but mobile users’ security concerns are not diminished as long as the associated behavioral factors are not understood and considered. Privacy is another users’ concern about mobile applications which mobile applications developers attempt to improve. In this study, we examine whether privacy-related factors can affect security perceptions about mobile applications. If privacy of mobile applications affect security, developers can devise the solutions to decrease these two significant concerns simultaneously and IS researchers better understand such interplay.

Keywords

Mobile applications, information security, privacy.

Introduction

As of 2014, 78 percent of global internet users are concerned about criminals hacking into their personal accounts (Statista 2014). The security issue is still a concern for technology users including users of mobile applications (apps) that are growing at a rapid pace. This challenge is relevant for both supply and demand sides (Liao and Cheung 2003; Bhatt and Bhatt 2016). For example, in a sensitive context such as mobile banking, users have frequently shown their concerns about the security of their accounts or channels through which they transact sensitive information (Federal Reserve System Board of Governors 2015). There are instances in which security issues disappointed the user to the extent they discontinued using new technology (Susanto et al. 2015).

Even though prior research on behavioral security studied security related phenomena, there is a need for further investigations on the factors affecting individual’s security perceptions in mobile apps context. In fact, recent works called for further research on antecedents of perceived security (Arpaci et al. 2015; and Ooi et al. 2016). Yet, the attempts have been limited to one of the followings: a) security is identified as a general perceived risk (Luo et al 2010; Al-Jabri and Sohail 2012; Susanto et al. 2015), and b) security is restricted to its technical dimensions rather than subjective aspects (Kim et al., 2010). Against this backdrop, we develop a theoretical model which predicts the factors that affect the users’ perception of security in the context of mobile apps. In particular, this study seeks to answer these research questions: (1) What factors affect mobile apps users’ perception of security? (2) Do privacy-related factors affect security perceptions about mobile apps? To answer these research questions, we review security and privacy literature and propose our research model. This work extends the literature on mobile app security by addressing the discussed gap. Furthermore, this could be used by mobile app developers to understand and resolve their customers’ security concerns.
Literature Review

Security needs to be defined and distinguished at two levels that the prior literature occasionally did so. Security has technical and behavioral aspects. Common sense implies that the more technical security is present the more behavioral security is perceived. Technical security refers to the existence of means that will prevent unauthorized access to a computer or a computer network, whereas subjective security which refers to the individuals’ perception that using an app would be risk-free (Carlos Roca et al. 2009; Shin 2010). Therefore, security means can be absent while the security perception exists or vice versa. Arpaci et al. (2015) propose a more accurate definition for perceived security in the mobile context, in which, perceived security refers to the degree to which one believes that smartphones are secure for transmitting sensitive information such as personal and financial information.

An extensive body of literature in the mobile context is dedicated to adoption—using TAM to develop models of mobile apps adoption (Gu et al. 2009; Zhou et al. 2010; Luo et al. 2010; Zhou 2011b). Although security issues did not hold organizations back from adopting innovative technologies into their routines such as smartphones, the security of these devices remains a major concern (Arpaci et al., 2015). Another stream discussed security and privacy using privacy calculus theory (Keith et al., 2013; Kehr et al., 2015). Users’ trust is another variable that is of importance in this domain because of its frequent appearance in the literature. In the mobile context, users’ trust has been studied extensively and the findings regarding how trust affect users’ perception are somewhat contradictory. For instance, firm reputation was found to have no relationship with trust to the firm’s mobile app (Gu et al. 2009; Kim et al. 2009), while other studies found strong support for relationship between firm reputation and trust in electronic environments, even across diverse cultures (Johnson and Grayson 2005; Eastlick et al. 2006; Jin et al. 2008).

Theory Development

Customers are not only worried about their financial transactions, but also their personal information which they share with their mobile apps. Additionally, organizations share the same concern as the customers, which is the insecurity of smartphones (Arpaci et al. 2015). If there is lack of security, individuals are less likely to use any mobile apps (Giovanis et al. 2012). We believe that in mobile apps context, the distinction between privacy and security is blur and privacy-related perceptions impact individuals’ perceived security about mobile apps (see figure 1). When customers have privacy concerns about using and transacting data with mobile apps, such concerns influence individuals’ view on the security of such apps.

Trusting Beliefs

We define trust as individual’s belief that the other party’s characteristics are beneficial (Susanto et al. 2015). The direct effect of trust on behavioral intention to adopt a new technology is well established (Roca et al. 2008; Shin 2010; Gu et al. 2009; Shen et al. 2010; Zhou 2011a). Nevertheless, in the mobile app context, the shortage of research and disagreements over the role of trust remains an issue. Shen et al. (2010) suggest trust affects security which is the mediator of trust and adoption intention. Similarly, we argue that having trust to an app could reinforce security perception of mobile apps because when individuals have trust on a mobile app they have less security concern about that app. Thus, we hypothesize:

H1: Trusting beliefs have a positive impact on the perceived security of mobile apps.

Perceived Effectiveness of Privacy Policy

Effectiveness of privacy policy is defined as the extent to which a customer believes that the privacy statements of mobile app provide accurate and reliable information about the associated developers’ information privacy practices (Xu et al. 2011). It is argued that the more effective a privacy policy is written and distributed by the mobile apps developer, the less risk is perceived by the individuals. Ponte et al. (2015) found a positive relationship between privacy/security policy and perceived security. In addition, the supported relationship from security policy to perceived security and perceived security to trust might suggest a direct relationship between the effectiveness of privacy policy and trust beliefs. We
believe when individuals read the security policy of a mobile app, their trust to that mobile app increases. Thus, we hypothesize that:

H2: Effectiveness of privacy policy has a positive impact on the perceived security of mobile apps.
H3: Effectiveness of privacy policy has a positive impact on trusting beliefs in mobile apps.

H4: Perceived privacy concerns have a negative impact on the perceived security of mobile apps.

H5: Improper access has a negative impact on the perceived security of mobile apps.
H6: Improper access has a positive impact on perceived privacy concerns of mobile apps.

We also adopt several control variables in our study based on privacy and security literature to examine the relationships of our model rigorously. We included age, gender, internet experience, invasion of security, and media exposure as the control variables in the proposed model.
Methodology

The target population of this study is mobile app users in the U.S. An online survey would be administered through Amazon Mechanical Turk. Prior literature emphasized that mTurk is reliable, easy to access, affordable, and superior to both the traditional data collection methods and other similar digital respondents’ pools (Kees et al. 2017). In designing the survey, we adopt the previously developed measures for perceived security, trust, privacy concerns, privacy policy effectiveness, and improper access from the prior literature. The process of data collection involves: (1) a preliminary pilot study with less than 50 mobile apps users (university students) to get feedback about the questions; and (2) distributing the revised survey on Amazon Mechanical Turk among mobile apps users so that we can collect data from mobile apps users with different gender, age groups, and educations. Finally, we use multivariate techniques, especially structural equation modeling (SEM) to analyze the research model after reliability and validity checks.

Discussion and Conclusion

The key objective of this paper is to develop and test a nomological model to understand what factors influence the security perceptions of mobile apps users. The model posits that perceived trust, perceived privacy policy effectiveness, perceived privacy concerns, and improper access affect mobile app users' security perception. We contribute to mobile apps security literature by employing privacy-related factors as the predictors of security perception. By mitigating the security concerns of mobile apps users, developers can eliminate barriers and hurdles that can change the users' decision to discontinue the use of mobile apps. We recommend that future researchers dedicate more attention to the role of security which seems to remain an issue as technology moves forward.

REFERENCES


