ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/328492218

# Mobile Applications Security: Role of Privacy

**Conference Paper** · January 2018

CITATIONS
8

READS
3,677

**3 authors:**

Hamid Reza Nikkhah
University of Nevada, Las Vegas
**13** PUBLICATIONS **291** CITATIONS
SEE PROFILE

Ali Balapour
University of Arkansas
**6** PUBLICATIONS **461** CITATIONS
SEE PROFILE

Rajiv Sabherwal
University of Arkansas
**166** PUBLICATIONS **11,651** CITATIONS
SEE PROFILE

All content following this page was uploaded by Hamid Reza Nikkhah on 24 October 2018.

The user has requested enhancement of the downloaded file.

# 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.

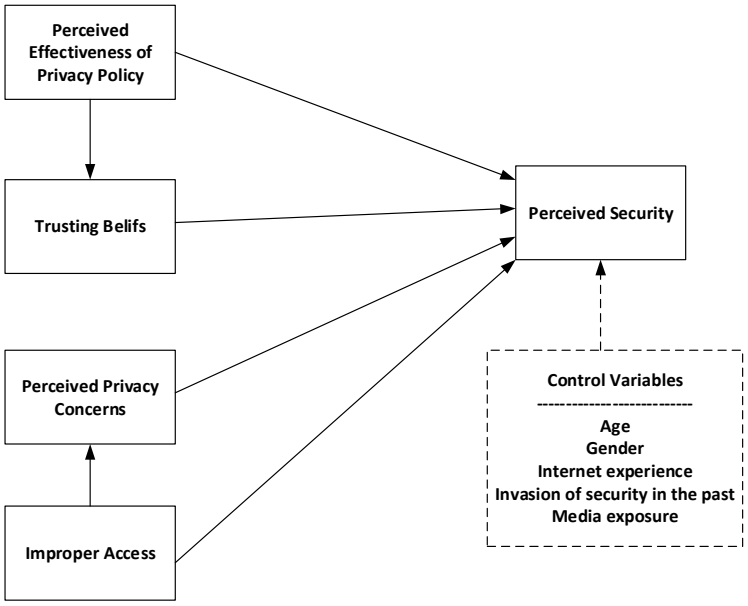


**Figure 1. Research Model**

## *Perceived Privacy Concerns*

Privacy is a multi-facet concept and there is not a unanimously agreed definition for it (Smith et al. 2011; Bélanger and Crossler 2011). Regarding the variety of definitions, privacy concern in our model is a subjective variable. Therefore, we define *privacy concerns* as "the ability of the individual to personally control information about one's self" (Smith et al. 2011; Smith et al. 1996). The interaction of privacy and security is nothing to be taken lightly since in different contexts the magnitude of their effects on intention to use is altered (Roca et al. 2008; Shin 2010; Ponte et al. 2015). Further, whether privacy is antecedent of security or vice versa is unclear in the literature as some studies aggregated them into a single construct while others applied them separately (Shin 2010). We believe that if customers' privacy concerns are elevated, they will perceive mobile apps insecure. So, we hypothesize that:
**H4:** Perceived privacy concerns have a negative impact on the perceived security of mobile apps.

## *Improper Access*

A significant aspect of customers' concern is related to their doubt about whether mobile app service providers have enough ability to prevent unauthorized access to their personal information (Smith et al. 1996; Zhou 2011b). Individuals are fully sensible of such threat to the extent that monetary incentives would not diminish their concerns about unauthorized access to their information which individuals share with a third party (Hann et al. 2002). Improper access is known for its effect on privacy concern, but we believe it also comes with an influence on perceived security (Smith et al. 1996; Zhou 2011b). By extension, we anticipate improper access negatively affects perceived security. Consequently, we hypothesize that:
**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

Al-Jabri, I. M., and Sohail, M. S. 2012. "Mobile Banking Adoption: Application of Diffusion of Innovation Theory," *Journal of Electronic Commerce Research* (13:4), pp. 379-391.

Arpaci, I., Yardimci Cetin, Y., and Turetken, O. 2015. "Impact of Perceived Security on Organizational Adoption of Smartphones," *Cyberpsychology, Behavior, and Social Networking* (18:10), pp. 602-608.

Arpaci, I., Yardimci Cetin, Y., and Turetken, O. 2015. "Impact of Perceived Security on Organizational Adoption of Smartphones," *Cyberpsychology, Behavior, and Social Networking* (18:10), pp. 602-608.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1042.

Bhatt, A., and Bhatt, S. 2016. "Factors Affecting Customers Adoption of Mobile Banking Services," *The Journal of Internet Banking and Commerce* (21:161), pp. 1-22.

Carlos Roca, J., José García, J., & José de la Vega, J. 2009. "The Importance of Perceived Trust, Security and Privacy in Online Trading Systems," *Information Management & Computer Security* (17:2), pp. 96-113.

Eastlick, M. A., Lotz, S. L., and Warrington, P. 2006. "Understanding Online B-To-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *Journal of Business Research* (59:8), pp. 877-886.

Federal Reserve System board of governors. 2015. "Consumers and Mobile Financial Services 2015" (available online at http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf; accessed August 22, 2017).

Giovanis, A. N., Binioris, S., and Polychronopoulos, G. 2012. "An Extension of TAM Model with IDT and Security/Privacy Risk in the Adoption of Internet Banking Services in Greece," *EuroMed Journal of Business* (7:1), pp. 24-53.

Gu, J. C., Lee, S. C., and Suh, Y. H. 2009. "Determinants of Behavioral Intention to Mobile Banking," *Expert Systems with Applications* (36:9), pp. 11605-11616.

Hann, I.-H., Hui, K. L., Lee, T., and Png, I. P. L. 2002. "Online Information Privacy: Measuring the Cost-benefit Tradeoff," in *Proceedings of the 23rd International Conference on Information Systems*, L. Applegate, R. D. Galliers, and J. I. DeGross (eds.), Barcelona, Spain, pp. 1-10.

Jin, B., Yong Park, J., and Kim, J. 2008. "Cross-Cultural Examination of the Relationships among Firm Reputation, E-Satisfaction, E-Trust, and E-Loyalty," *International Marketing Review* (25:3), pp. 324-337.

Johnson, D., and Grayson, K. 2005. "Cognitive and Affective Trust in Service Relationships," *Journal of Business research* (58:4), pp. 500-507.

Kees, J., Berry, C., Burton, S., and Sheehan, K. 2017. "An Analysis of Data Quality: Professional Panels, Student Subject Pools, and Amazon's Mechanical Turk," *Journal of Advertising* (46:1), pp. 141-155.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607-635.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Aactual User Behavior," *International Journal of Human-Computer Studies* (71:12), pp. 1163-1173.

Kim, C., Tao, W., Shin, N., and Kim, K. S. 2010. "An Empirical Study of Customers' Perceptions of Security and Trust in E-Payment Systems," *Electronic Commerce Research and Applications* (9:1), pp. 84-95.

Kim, G., Shin, B., and Lee, H. G. 2009. "Understanding Dynamics between Initial Trust and Usage Intentions of Mobile Banking," *Information Systems Journal* (19:3), pp. 283-311.

Liao, Z., and Cheung, M. T. 2003. "Challenges to Internet E-Banking," *Communications of the ACM* (46:12), pp. 248-250.

Luo, X., Li, H., Zhang, J., and Shim, J. P. 2010. "Examining Multi-Dimensional Trust and Multi-Faceted Risk in Initial Acceptance of Emerging Technologies: An Empirical Study of Mobile Banking Services," *Decision support systems* (49:2), pp. 222-234.

Ooi, K. B., and Tan, G. W. H. 2016. "Mobile Technology Acceptance Model: An Investigation Using Mobile Users to Explore Smartphone Credit Card," *Expert Systems with Applications* (59), pp. 33-46.

Ponte, E. B., Carvajal-Trujillo, E., and Escobar-Rodríguez, T. 2015. "Influence of Trust and Perceived Value on the Intention to Purchase Travel Online: Integrating the Effects of Assurance on Trust Antecedents," *Tourism Management* (47), 286-302.

Roca, C. J., García, J. J., and de la Vega, J. J. 2009. "The Importance of Perceived Trust, Security and Privacy in Online Trading Systems," *Information Management & Computer Security* (17:2), pp. 96-113.

Shankar, A., and Kurami, P. 2016. "Factors Affecting Mobile Banking Adoption Behavior in India," *The Journal of Internet Banking and Commerce* (21:160), pp. 1.

Shen, Y. C., Huang, C. Y., Chu, C. H., and Hsu, C. T. 2010. "A Benefit–Cost Perspective of the Consumer Adoption of the Mobile Banking System," *Behaviour and Information Technology* (29:5), pp. 497-511.

Shin, D. H. 2010. "The Effects of Trust, Security and Privacy in Social Networking: A Security-Based Approach to Understand the Pattern of Adoption," *Interacting with computers* (22:5), pp. 428-438.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1016.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996 "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Statista. 2014. "Share of Global Internet Users Who Are Concerned about Criminals Hacking into Their Personal Bank Accounts as of November 2014, By Country" (available online at http://www.statista.com/statistics/373422/global-opinion-criminal-hacking-personal-bank-account/; accessed August 29, 2017).

Susanto, A., Chang, Y., and Ha, Y. 2016. "Determinants of Continuance Intention to Use The Smartphone Banking Services: An Extension To the Expectation-Confirmation Model," *Industrial Management and Data Systems* (116:3), pp. 508-525.

Zhou, T. 2011a. "An Empirical Examination of Initial Trust in Mobile Banking," *Internet Research* (21:5), pp. 527-540.

Zhou, T. 2011b. "The Impact of Privacy Concern on User Adoption of Location-based Services," *Industrial Management and Data Systems* (111:2), pp. 212-226.

Zhou, T., Lu, Y., and Wang, B. 2010. "Integrating TTF and UTAUT to Explain Mobile Banking User Adoption," *Computers in Human Behavior* (26:4), pp. 760-767.



View publication stats