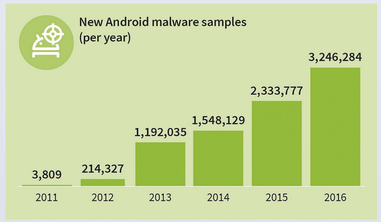
Implications of Mobile Application Security, Application Features and Consumer Adoption

Eralda Caushaj, Anne Kohnke, & John Zhu, *with Graduate Research Assistants*: Xi Li, Rahul Mamindla,
Mohamadali Rihan, Jiayi Sun, Varun Vikram
Lawrence Technological University
College of Business + IT

Project Summary

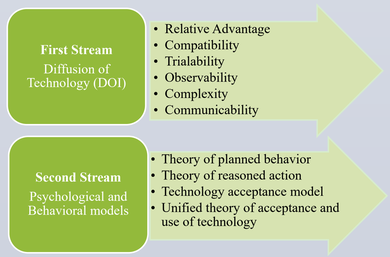
The focus of this research is to understand the impact of mobile software application security permissions and application features on the consumer adoption of Android smartphone applications. In November 2016, Android captured a record 88% of the global marketshare in smartphone operating systems (Sui, 2016). With the increase in this smartphone marketshare, applications developed and made available in the Android Market (Google Play), alternative online shops, and third-party developers has exponentially increased. Unlike applications published in the Apple or Marketplace (Microsoft) stores, the applications published in Google Play do not need approval from Google but they do need to be signed by a private key so that ownership can be verified. With the increase of mobile app popularity coupled with the saturation of smartphone devices, two areas of study attract the attention of both business practitioners and academic scholars: mobile app security and mobile app adoption (Caushaj et al., 2017; Caushaj et al., 2017).

There are two main security concerns for mobile apps, which has been the focus for research on mobile cybersecurity: malware and advertisements. Malware steals and misuses information by using permissions or phishing, which violates the user data privacy (Unuchek and Chebyshev, 2016). Ad networks may pose a threat to the user data privacy when they gain access to user profile information using permissions without making them aware to users (Stevens et al. 2012). In practice, in order to properly function, legitimate mobile apps, advertisements (ads), and malware all require access to mobile data and resources. As such, it is hard for a normal user to make optimal decisions to maximize the value of security and functionality. Nor are they fully aware of the collection and use of the personal data that ad networks access. The ad networks or malware are therefore able to put the user in greater danger by requesting permissions that are not necessary for the functionality of the app. When a user sends a request with personal information to a legitimate app, this information is stored on an application server, with a separate copy passed to and stored on a malware/ad server. Researchers in this domain study the Android permissions system and Android malware detection to develop relevant tools for this purpose (e.g. Caushaj et al., 2017a, b; Ferreira et al. 2015; Sarma et al. 2012; Zhou et al., 2012).



In comparison, professionals in marketing and strategic management gravitate toward the user acceptance and use of mobile apps. The theoretical disciplines supported by the development of these theories such as information technology, marketing, sociology, and psychology concentrate on two streams of exploration: the determination of users' adoption and usage of mobile apps. The first stream rests on the theory of the diffusion of technology (DOI) and takes the perspective of innovation attributes, i.e. relative advantage, compatibility, trialability, observability, complexity, and communicability (Roger 2003). The other stream uses psychological and behavioral models, such as the theory of planned behaviour (TPB) (Ajzen, 1991), the theory of reasoned action (TRA) (Ajzen and Fishberin, 1980), the technology acceptance model (TAM) (Davis et al., 1989; Davis, 1989), and a more comprehensive unified theory of acceptance and use of technology (UTAUT) (Venkatech et al. 2003, 2007, 2012). By combining multiple theories together researchers aim to exploit the motivation and intention side of technology adoption (Kohnke, Cole, & Bush, 2013). This school of research takes the perception of consumers' utilitarian benefits of mobile apps such as mobility, usefulness, communication, etc. as well as hedonistic benefits of pleasure, self-efficacy, entertainment, or enjoyment and contributes to revealing the mechanism through which mobile apps serve as a medium to fulfills consumers' various personal needs (Yang 2015).

Despite the popularity of mobile app, there is a significant gap in research that focuses on the relationship between mobile app security and adoption decisions of mobile apps. Research on these two topics are largely advanced paralleled and there lacks study to integrate them into one framework to thoroughly understand user adoption for mobile app.

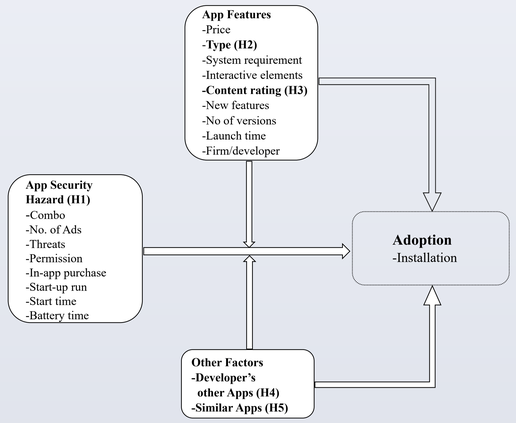


Conceptual Framework

Specifically, we will explore the following questions: First, what is the current state of mobile app security concerns? Second, among other conventional drivers for mobile apps, how does app security influence consumers' adoption decisions? Third, compared to other conventional determinants of mobile app adoption, how impactful is the effect of app security? Fourth, what are the contingencies (boundary conditions) for the effect of app security on consumers' adoption decision?

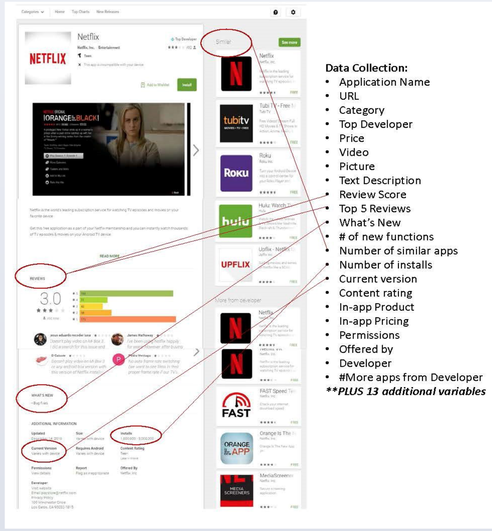
Our study will bridge the research gap in the domain of information technology and consumer research. We developed a conceptual framework to test the effect of app security on consumer adoption of mobile app. We will empirically test our comprehensive conceptual framework on the leading Android mobile apps in the Google Play platform. This includes the top 30 most downloaded mobile apps within each category, which includes more than 1,800 popular paid or free mobile apps. Figure 2 below demonstrates an example of a mobile app in the Google Play Store and some of the information we plan to collect, which maps to our framework in Figure 1.

Figure 1. The following conceptual framework was developed to guide this study:



Note:
- H1 is the main effect of App Security Hazard on App Adoption
- H2-H5 are the moderating effects on the main effect in H1
- App Security information will be partially acquired based on the approach proposed in Caushaj et al., 2017
- Other Relevant information is publicly available and obtainable from the Android App webpage via Google Play.

Figure 2: Example Mobile App - Netflix



Drawing on the literature of mobile app security and app adoption, we developed and plan to test a number of hypothesis, which we summarize as follows:

Security hazards tend to lower the perceived value of mobile apps. The potential malware poses direct threats to mobile functioning and usage such as information access, communication, mobility, ease of use, and the hardware operations for smartphones and tablets. In a similar vein, the privacy invasion may trigger malicious behaviors toward user and user experiences as well. Consequently, the hedonic value of the mobile app decreases as with the poor utilitarian performance as reflected in the lost pleasure and joy in entertainment, the emotional attachment, the sense of achievement component, especially in gaming and social media apps consumption (Liu, 2006; Strahilevitz, 1999). As such, we hypothesize:

H1: App security hazard has a negative impact on mobile app adoption.

We further identify a number of moderators for the proposed negative relationship. For hedonic mobile apps, in the category of gaming, entertainment, and social media apps consumption, the high level of hedonic benefits will compensate partially the potential loss of perceived value due to poor app security. As such, users tend to lower the requirement for app security in decision making for app adoption. Therefore,

H2: For hedonic mobile apps, the negative effect of app security hazard on app adoption is weaker.

High quality apps will provide superior utilitarian benefits such as information access, communication, mobility, ease of use, etc. The outstanding utilitarian benefits counteract the negative value assessment of potential app security concerns. As such, users are inclined to loosen the requirements for app security in app evaluation and adoption. Therefore,

H3: For quality mobile apps, the negative effect of app security hazard on app adoption is weaker.

Signaling theory (Spence, M. 1973) suggests that reputable developers signal low likelihood of vulnerable safety loopholes in developed software and low likelihood of misconduct by the developer with user information, as well as the low perceived functional, financial and psychological risks (Walter, Gupta, & Su, 2006). Therefore, user concerns on app security will be attenuated if the app is developed by a reputable developer.

H4: For apps developed by reputable developers, the negative effect of app security hazard on app adoption is weaker.

If there are abundant substitutes on market it is relatively easy for users to select a mobile app with similar utilitarian benefits but with better security features. Therefore, users will be more stringent on the requirements for app security. As such,

H5: For apps with more substitutes, the negative effect of app security hazard on app adoption is stronger

Literature Review

App Security

The permission system in the Android OS governs an app's access to information of users. Legitimate mobile apps, advertisement networks, and malware threats all require data access to mobile resources and personal information for installation and proper function. Permissions are classified into three different protection levels, i.e. normal, dangerous, and signature (Android Developers, 2016). Apps must request the appropriate permissions to utilize additional system capabilities access or user information.

Minimizing the privacy risk associated with Android apps is difficult, because it is unlikely for an average user to have sufficient knowledge about security to make informed decisions.

Malicious applications and privacy-invasive ad networks are the most common concerns for mobile security because they may lead direct or indirectly to malicious activities toward mobile user and devices. They have certain sets of permissions that they require in order to operate, but which permissions are required varies depending on the type of information or functionality being misused.

As new methods and exploits are discovered, mobile malware and adware become the major threats to Android users. According to Kaspersky Lab (Unuchek and Chebyshev, 2016), in 2015 alone, they identified over 880,000 new malicious programs targeting at mobile devices, as many as three times the number of 2014. These programs include Trojans that steal and distribute the user's online account credentials, and ransomware that hijack a user's device and force them to pay ransom for unlocking. The official Google Play store secreted developed a protective program, named Bouncer, to screens all incoming apps for malware with (Lockheimer, 2016). However, there have been multiple incidents Bouncer was fooled and allow malware-infected apps to sneak through into the store.

Advertisements are able to use mobile app permissions to collect user's proprietary data and send it to advertisement servers without user knowledge or consent (Steven et al. 2012). In this way, the users' control for privacy is neutralized. Many Android apps rely their revenue on in-app advertising, which generally are provided by different advertising networks, ranging from Google's extremely popular AdMob to numerous small networks used in only a few applications. App developers integrate ad networks into their mobile apps by using ad libraries provided by the networks. In practice, app developers simplify the process of ads incorporation by using API provided by ad library for ad display. Many ad libraries require sets of special permissions, and ask developers to include permissions beyond what are necessary for app's normal function in order to use the desired app library. The ad libraries further gain automatically grant for any permissions the host app is entitled, a property that compromises the privacy of the user.

Studies have been focusing on the Android permission system and Android malware detection and tools develop. Zhou et al. (2012) developed an approach for Android malware detection which first filters the apps by removing the apps without risky permission combinations, and then compares the apps' behavioral footprints with those of known malware. Sarma et al. (2012) and Peng et al. (2012) proposed evaluation mechanism and models using multiple different risk signals based on permissions requests of an app. Securacy (Ferreira et al. 2015) is developed as a user-driven approach to educate users about Android security. Similarly, Kirin serves as a tool that performs static analysis and blocks apps that declare risky permission combinations. Yang et al. (2015) introduces AppIntent, a tool to analyze apps using guided symbolic execution to locate the origins of sensitive data transmission. Caushaj et al., 2017 have implemented the Android Application Permission Manager (AAPM) to educate and inform users and help prevent them from installing malicious apps.

Selected References

Ajzen, I. and Fishbein, M. 1980. Understanding Attitudes and Predicting Social Behaviour, Prentice-Hall, Englewood Cliffs, NJ.

Ajzen, I. 1991. "The Theory of Planned Behavior," Organizational Behavior and Human Decision Processes, 50 (2), 179-211.

Caushaj Eralda, Rahul Chandrashekar, Veera Raju, Sai Praveen, Katherine Schwartz, Huirong Fu, Ishwar Sethi, Ye Zhu. 2017. "Android Application Permission Manager (AAPM): Classification and Security Assessment for Android Apps," Working Paper.

Kohnke, A., Cole, M.L., & Bush, R. (2013). "Incorporating UTAUT Predictors for Understanding Home Care Patients' and Clinician's Acceptance of Healthcare Telemedicine Equipment" Journal of Technology Management & Innovation, 9(2), 29–41.

Stevens R., C. Gibler, J. Crussell, J. Erickson and H. Chen. 2012. "Investigating User Privacy in Android Ad Libraries," IEEE Mobile Security Technologies (MoST), San Francisco, CA, May 24, 2012.

Unuchek R. and V. Chebyshev, 2016. "Mobile malware evolution 2015", Securelist, 2016. [Online]. Available: https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/. [Accessed: 13- Jun- 2016].

Venkatesh V, C Speier, and MG Morris. 2007. "User acceptance enablers in individual decision making about technology: Toward an integrated model," Decision Science., 33, 297–316.

Yang Z., M. Yang, Y. Zhang, G. Gu, P. Ning and X. Wang. 2013. "AppIntent: Analyzing Sensitive Data Transmission in Android for Privacy Leakage Detection," in Proc. ACM SIGSAC Conf. on Computer & Communications Security. 1043-1054.

Zhou Y., Z. Wang, W. Zhou, and X. Jiang. 2012. "Hey, You, Get off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets," NDSS, 2012.