Mobile Security

Kent Tabada
Georgie Recabo
Jemwel Dela Peña

Abstract

Mobile devices have become a vital part of our daily lives in recent years. These have proven to be a beneficial scientific invention that efficiently meets personal and business needs. Because of the wide range of mobile devices and critical apps offered by mobile device manufacturers, the availability of mobile services has dramatically risen in this period. At the same time, both manufacturers and users are confronted with a slew of mobile security challenges and data privacy threats. Therefore, mobile devices are an ideal target for various security issues and data privacy threats in a mobile ecosystem.

In this paper, we provide a literature of the security challenges, perspective on mobile security, and vulnerabilities of a mobile ecosystem. Furthermore, we discussed some key points required to ensure mobile security and defend against data privacy threats. Also briefly discussing what the mobile security about and what is the best practice on doing and what best use in terms of security on mobile

Introduction

Smartphones, tablets, laptops, and other portable computing devices, as well as the networks to which they connect, are protected from risks and vulnerabilities associated with wireless computing by mobile security.

As the number of devices and the ways in which they are used has grown rapidly, securing mobile devices has become increasingly crucial. This is especially problematic in the workplace when employee-owned devices connect to the corporate network. Increased corporate data on devices attracts cybercriminals, who can use mobile malware to target both the device and the back-end systems they access. IT departments work to make sure that employees are aware of the permissible use regulations, and that administrators follow them. Organizations might be subject to malicious malware, data leakage, and other mobile dangers if they do not implement mobile device security safeguards. If systems must be shut down, security breaches can create extensive corporate interruptions, including disrupting IT operations and decreasing user productivity.

Literature

According to Wu D, Moody G, Zhang J et al. (2020) on their study the Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention it was revealed that the rapid global usage of mobile programs (also known as apps) has raised security and privacy concerns. Users of mobile apps often have a poor grasp of information security, and they frequently ignore security messages intended to improve app security. We explore how security perceptions of apps are generated and how these perceptions influence users' intentions to continue using apps by addressing both mobile app UI usability and mobile security notification (MSN) design. As a result, we devised and carried out a series of controlled survey studies with 317 individuals in various MSN interface scenarios, varying the types of MSN interfaces (high vs. low disruption), the context (hedonic vs. utilitarian scenarios), and the degree of MSN intrusiveness (high vs. low intrusiveness).

We discovered that both the usability of the app UI and the design of MSNs have a substantial impact on users' perceived security, which has a good impact on users' intention to continue using the service. Furthermore, we discovered a significant problem: disruptive MSNs, a typical method of delivering MSNs, annoy consumers and significantly impact their perceptions of app security. As a result, our findings directly contradict existing practice. If these findings hold true, current practice should move away from MSNs that cause task interruptions.

As stated by Weichbroth P, Łysik Ł. (2020) Mobile Security: Threats and Best Practices. Due to the continual discovery of new mobile device vulnerabilities, communicating mobile security dangers and best practices has become a top priority. The purpose of this article is to identify and assess existing dangers and best practices in the domain of mobile security in order to deal with this overarching issue. We conducted a literature review based on a set of keywords to this end. In the domain of mobile security, the collected results address known dangers and established best practices. This result was then presented to mobile app users (n = 167) via a survey instrument for their consideration.

To this purpose, the findings reveal a high level of awareness of hazards and countermeasures in the context of mobile applications. While acknowledging the risks connected with physical and social variables, the majority of respondents stated that harmful software and social-engineering schemes are mitigated by built-in mechanisms. The findings of the study contribute to the theory of mobile security by identifying and exploring a number of topics, both risks and best practices. Apart from that, this body of current knowledge has practical relevance, as evidenced by its applicability at both the individual and corporate levels. Furthermore, we propose that leveraging the security of mobile applications requires an awareness of the elements influencing users' intentions and motives to adopt and employ specific technologies. As a result, future work will focus on recognizing and modeling consumers' impressions of mobile app security and usability.

As stated by Yao M, Chuang M, Hsu C. (2018) on their study the Kano model analysis of features for mobile security applications that more than 200 mobile security applications (MSAs) with a variety of capabilities are available in the Google Play app store. With the Kano Model two-dimensional questionnaire, this study combines and extracts 12 key mobile security and antivirus features from the top 25 MSA manufacturers to see how consumers rate and define quality criteria for these features. The results of the analysis suggest that all features are either one-dimensional or indifferent in quality. Based on the SI and DSI values assigned to each feature for its impact on customer satisfaction, these 12 characteristics might be further divided into 5 quality kinds (O, OA, OI, IO, and I).

"Malware prevention," "safe surfing," "parental control," and "privacy protection" are the top four features that have the most impact on consumer happiness. These four aspects should be highlighted by MSA vendors. Because they have little impact on consumer happiness, the "secure app advisor" and "app lock" may receive less attention. "Data backup," "junk file cleanup," "Wi-Fi security," "message and call filter," "remote erase," and "remote lock and find" all have a greater influence on enhancing customer happiness than on decreasing displeasure. To increase customer satisfaction, MSA providers with above-average quality must devote greater design effort to these characteristics. "Remote lock and locate" and "Wi-Fi security" are more important to female users, while "garbage file cleanup," "remote lock and locate," and "secure app advisor" are more important to users with less technological understanding.

According to Thompson N, McGill T, Wang X. (2017) in their study “Security begins at home”: Determinants of home computer and mobile device security behavior it was revealed that Users of personal computers are exposed to information security threats because they must make decisions about how to secure themselves on their own, frequently with little knowledge of technology or its ramifications. Personal computing users, on the other hand, are underrepresented in security research studies, particularly when it comes to mobile device use. The study detailed in this paper fills this knowledge vacuum by analyzing data from 629 home computer and mobile device users in order to better understand security behavior in both environments.

By considering the functions of social influences and psychological ownership, as well as actual conduct, the study model extends protection motive theory. The model was evaluated independently with home computer and mobile device users, and the results show that several of the predictors of security behavior differ between the two. Perceived vulnerability, self-efficacy, reaction cost, descriptive norm, and psychological ownership all influenced personal computing security intentions and behavior in both home and mobile device users, according to the findings. However, only perceived severity was found to influence mobile device security behavior, and neither response efficacy nor subjective norm had any effect on security intents for either type of user. These findings are examined in terms of their practical and scientific consequences, as well as the potential for new study in the area of personal computing security.

As stated in Stiakakis E, Georgiadis C, Andronoudi A. (2016) on their research about Users’ perceptions about mobile security breaches that Apart from the technology aspect of mobile device and application security, the economic aspect has been gaining increasing academic and industry interest. The purpose of this study is to look into how mobile users think about the economic impact of security breaches. Instead of looking at mobile users as a whole, Brandtzg's mobile user typology was used to look at them as various user types. (1) irregular users, (2) socializers, (3) entertainment type users, (4) instrumental users, and (5) advanced users are the five sorts of users.

A survey of smartphone and tablet owners was undertaken as part of the research portion of this study. The five user types in our sample were defined using particular classification rules based on the number and variety of mobile services used. The attitudes of mobile users were evaluated in terms of ten different types of security breaches.

The findings revealed that different user categories perceive the economic impact of security breaches differently, emphasizing that designing security rules and/or developing tools solely for the community of users is not the best strategy. Our study could add to the body of knowledge concerning mobile users and their views of security breaches. The findings of this study could be used by mobile content providers and developers to review and, if necessary, adapt their current techniques to fulfill users' security concerns.

As reported by Bitton R, Finkelshtein A, Sidi L et al. (2018) on their study Taxonomy of mobile users' security awareness that Smartphones are appealing to attackers who want to harvest sensitive information due to their popularity and the amount of important and private information they store. Exploiting human weaknesses (i.e., social engineering) is a common method for accomplishing this goal. Improving user security knowledge is a good way to protect against social engineering attacks. While user security awareness is reasonably high in the realm of personal computers (PCs), past research have indicated that security awareness is much lower in the mobile platform. A mobile user's skills for securely interacting with his or her smartphone are distinct from those required for safe and responsible PC use. As a result, mobile consumers' understanding of security concerns is a crucial part of information security.

Summary of Findings

Nowadays, mobile phones are frequently used, and this has resulted in an increase in security and privacy concerns. It's possible that the user has a poor understanding of how mobile security works. One thing is to identify and assess current dangers and best practices in the mobile security arena. Also, malware prevention, safe surfing, parental control, and privacy protection should be prioritized in mobile security applications (MSAs), as these provide greater user satisfaction in terms of mobile security.

The economic relevance of security breaches is seen differently by different user categories, meaning that designing security rules and/or developing tools solely for the community of users is not the best approach. And improving user security knowledge is a good way to protect against social engineering attack

Peers Evaluation

Evaluation Criteria	Group member: **Kent Tabada**	Group member: **Georgie Recabo**	Group member: **Jemwel Dela Peña**
Attends group meetings regularly and arrives on time.	5	5	5
Contributes meaningfully to group discussions.	5	5	5
Completes group assignments on time.	5	5	5
Prepares work in a quality manner.	5	5	5
Demonstrates a cooperative and supportive attitude.	5	5	5
Contributes significantly to the success of the Activity	5	5	5

References

https://www.sciencedirect.com/science/article/pii/S0167404818303341

https://www.mendeley.com/catalogue/612708a6-a3eb-304b-8fab-776c7c3c6ee4/

https://www.mendeley.com/catalogue/15c10bc4-dc43-3287-8f6f-a1c07371a177/

https://www.sciencedirect.com/science/article/pii/S0167404817301426

https://www.mendeley.com/catalogue/c03a7be3-fea0-3265-88d2-3781559a5014/