SAMPLE MANUSCRIPT

Android Security problem a necessity for the security of mass

1st Author	2nd Author	3rd Author
1st author's affiliation	2nd author's affiliation	3rd author's affiliation
1st line of address	1st line of address	1st line of address
2nd line of address	2nd line of address	2nd line of address
Telephone number, incl. country code	Telephone number, incl. country code	Telephone number, incl. country code
1st author's E-mail address	2nd E-mail	3rd E-mail

ABSTRACT

The current study has incorporated a brief analysis of the mobile security and data protection concerns with the growing pace of the technology. Moreover, easy access and equivalent facilities to a desktop has enabled the users to avail the mobility of technology so that it could minimise the time consumption and idle period of work. The report has initially incorporated the concept and necessity of mobile security followed by the threats the mobile users are facing with rapid improvement in mobile technology and number of applications. It has been observed that vulnerability of the mobile security has been hiked with the improved configurations and complexities in both the windows and android devices. Moreover, different applications contain such vulnerable threats spreading through mobile and attack the computers finally through data transfer. In that case, the research is going on regarding the threats to resolve the issue to the extent it could be.

General Terms

Your general terms must be any of the following 16 designated terms: online security, threats, viruses, malware, shield, technology, application, programme, software.

Keywords

Keywords are your own designated keywords.

1. INTRODUCTION

Data protection and security has become one of the prime objectives of the mobile users as mobility has become the key features in terms of professional and personal activities. The current study has incorporated the analysis of mobile security and its vulnerabilities hindering the natural process of mobile operation and store of data in the devise. The prime research question for this study would be:

- What is the necessity of security in android mobile and how is it executed for a better protection?

PhD Writing Assistance

WhatsApp number: +60-14-639 8196

URL: https://www.phdwritingassistance.com/

The current status of the mobile market has on a boom in presence of the improved technology and further scope of the technical development. Therefore, the vulnerability of the viruses and malware has been increased significantly over the past. With the improved mobile devices and operating system in the same, the number and strength of the new threats have been hiked over the previous threats. A number of researches have been performed on this issue and therefore, solution has been developed accordingly. However, with the rapid growth in the technological pace, the complexity in mobile threat has also been increased over the time. The key purpose of the current study is to investigate the current scenario regarding the mobile security and its probable solution to resolve the issues to some extent. Initially the necessity and concept of mobile threat has been explained followed by the mobile threats, found from most of the users. The later part of the study has entailed with the probable solution of this issue in order to protect the dives from virus attack so that the saved documents and confidential files would be saved from its deletion and other damages.

2. NECESSITY OF MOBILE SECURITY

Mobile has become the prime storage device and thus, an important gadget to store both the personal and professional data in mobile. Therefore, security of the personal data is an important concern now a day in presence of the technical improvement and thus, advanced process of data leakage practices. Therefore, mobile security has become one of the key elements among the people. Both the personal and professional data are being saved in the mobile due to the nature of mobility. Therefore, an effective security application would secure the data complying with the data security issue. Moreover, data transfer mechanism has also increased the vulnerability of the device damage and crash of the application software. According to author, mobile security ensures data protection practices that restrict the leakage of the data and piracy of the same [1]. In that case, the plethora of data, as

exchanged through mobile devices has increased the vulnerability of the data transfer. In that case, most of the financial and other business data are at the vulnerable position as these types of data are transferred most of the time.

Figure 1. Mobile Security

3. SPREAD OF VIRUS

The cell phone virus attacks the mobile phone through data transfer via email attachments, Bluetooth file transfer and internet downloads that in turn multiplies itself while capturing the space in secondary storage through removing important documents. Therefore, virus spread is happened through replication of programming which therefore attached to the operating system and thus, moved via any of the transfer channels. In this context, author stated that with the increasing scope of technological development and presence of improved data transfer channel, the vulnerability of the devices has been increased through mobile-to-mobile data transfer through the above mentioned channels [2]. The operating system of an android device itself is protected from any type of virus and malware. Thus, the scope of virus attack in android phone is minimal. All android phones possess the feature as the locked boot leader that resists the access of partition. Therefore, multimedia messaging is the only way of spreading mobile virus.

..

4. THREATS AGAINST MOBILE SECURITY

Threats against the mobile security include viruses and malware sourced from different devices and spread to the mobiles. However, the severity of the viruses and malware has been increased in presence of the advanced technology and innovative software application [3]. It has also been observed that every virus is associated to a particular software or operating system which is developed to protect the same while proven to be harmful for the other devices. Cabir is the first mobile virus detected from the first generation multimedia devices. However, based on the current

sets of viruses and malware, Cabir is comparatively less vulnerable in case of the effects on the secondary storage devices. In case of an android device, unlocked boot leader and side loading are the only ways that the android phones are bing affected from the malware. However, these options are by default locked in phone. On the other hand, the malware issue might come due to the disabled state of some mobile feature that would protect the operating system from malware attack.

5. RECENT TREND OF MOBILE MALWARE

There has been a significant increment in malware and effectiveness of the same over the devices. In the opinion of scholars, the level of harmfulness of malware is comparatively higher than the viruses due to features and programming of the software [4]. According to the recent statistics, there has been a steady growth in malicious programming in the SMS domain where the mobile Trojan infections in nature where the mobile devices, configured with python or java possesses the vulnerability of suffering from this threat. The growth in IQC spams and while increment in total number of Wap sites have been observed during the recent decades. During the year of 2008, Symbian malware has attained a significant market share as it has been developed as the spy of user's mobile devices where the developer company has attained a huge profit from this malware programme. In this context, the windows system has drawn a special attention in malware attack where Duts and Brador are two serious malware, developed for the windows devices.

Figure 2. Applications carrying out threats

6. RISK FROM THE ATTACK OF MOBILE VIRUSES

.

Risk of mobile virus is comparatively higher than the other devises. In that case, it has been observed that devices like computers and laptops are configured with an improved operating system where the resistance and protective action in those devices

would easily be taken against the same. However, in case of mobile devices the scope of such protection is significantly less and thus, the vulnerability of the devices in case of affecting the same is significantly higher in comparison of the other devices accessible to the users. Moreover, the data transfer in mobile devices is faster and wider due to its user friendliness [5]. Comparatively, the data transfer among devices like computers and laptop is highly complex in nature and costly. Moreover, operation through mobile devices have been replaced the other devices due to its operational ease and mobility. Thus, the risk profile associated to the mobile devices is therefore, higher due to availability of transfer media available in windows and android devices.

7. MEASURES TO BE ADOPTED

Protection is a necessary measure to resist the data destruction and transfer of the vulnerable content over the mobile devices. The initial and most popular measure for protecting devices from viruses and malware is antivirus and antimalware functions that would protect the devices from the virus attack. The conventional protection has been to detect and remove the vulnerable elements from both the desktops and laptops where the new types of antivirus protects the mobile devices through blocking the vulnerable sites and sources and resist the users to access the same. Therefore, prevention has been strict in new protections than detection from the affected devices. As a reason, some of the viruses and malware would damage the device and erase important data faster than the detection. In that case, the shield could not work properly as the malware could have replicated in a vast area of the storage and erased all data stored. An android device is protected itself through its operating system. Instead, cache memory is the option to remove the virus and malware. For further protection Bitdefender is the best option to protect android device from virus and malware/

8. CONCLUSIONS

From the above discussion, it has been observed that mobile security has become the key concern as the utilisation of this devise in present of the improved configuration is comparatively higher than the other devices. The reason would be defined as the mobility and easy access of the online channels for data transfer and access. However, mobile threats would be vulnerable in case the mobile does not have any protection in terms of antivirus and malware shield. In that case, the users need to protect the device from severe attack through installation of a sound and authentic shield for better utilisation and security compliance..

9. ACKNOWLEDGMENTS

10. REFERENCES

.

[1] Mollah, M.B., Azad, M.A.K. and Vasilakos, A., 2017. Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications*, *84*, pp.38-54..

[2] Faria, N.R., Sabino, E.C., Nunes, M.R., Alcantara, L.C.J., Loman, N.J. and Pybus, O.G., 2016. Mobile real-time surveillance of Zika virus in Brazil. *Genome medicine*, *8*(1), p.97..

[3] Roman, R., Lopez, J. and Mambo, M., 2018. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, *78*, pp.680-698..

[4] Feizollah, A., Anuar, N.B., Salleh, R. and Wahab, A.W.A., 2015. A review on feature selection in mobile malware detection. *Digital investigation*, *13*, pp.22-37..

[5] Mahaffey, K.P., Buck, B.J., Robinson, W., Hering, J.G., Burgess, J.D., Wyatt, T.M., Golombek, D., Richardson, D.L., Lineberry, A.M., Barton, K. and Evans, D.L., 2017. *Methods and systems for sharing risk responses between collections of mobile communications devices*. U.S. Patent 9,781,148..

.