Security Management

Mohammed Alhazzaa

Abstract— Mobile devices such as mobile phones and tablets have gained acceptance around the world with many adopting the same for everyday use. It is difficult to imagine a world where there are no mobile communication devices. Especially now the most of the activities people engage in are to some extent tethered to the use of mobile communication devices. The rapid adoption of this technologies is however associated with the increased potential for data loss making the aspect of security an important consideration when choosing a device. Unfortunately, data security is still a concern requiring improvements and possibly innovations to ensure safe use of these important devices.

Index Terms— Communication, Management, Safety, Security, Systems, Technology.

1 Introduction

OPERATING system and device security is a topic that many mobile device users consider when choosing tablets and mobile phones. The fact that mobile devices have gained popularity and consequently have high acceptance levels around the world makes the aspect of information integrity and security a central consideration when choosing a device that one can confidently use without the fear of information loss or even risking access to the same by unauthorized third parties. Mobile devices are taking up the role of computers, personal organizers, and even data storage tools consequently making them very important tools for the modern human being. The idea of unauthorized third parties having the ability to access and even retrieve information from these devices without the consent of the owners makes the aspect of security important when choosing mobile devices to invest in (Willems, 2013). The cost and features presented by the android operating system make it ideal as a system for use in everyday applications. The fact that Android is developed based on the Linux platform makes it an ideal choice for mobile device manufacturers who want flexibility and the ability to port the operating system to suit various mobile device hardware. Operating systems like the iPhone operating system (ios) associated with Apple corporation is considered secure and the least susceptible to hacking or infiltration by malicious code as it is developed around selected hardware built by the proprietor of the said hardware. This makes the operating system more secure than the Windows and Android platforms that provide their source code to various device manufacturers, who then provide the same to third parties that act as application developers for the said companies. The outcome is source code that is present in the public domain making it relatively easy to access for purposes of reverse engineering and alterations to fit into various devices (Willems, 2013).

Mobile devices running various versions of the Android operating system are currently present in the global marketplace with device manufacturers seeking to provide as many features as possible to the public. The fact that mobile devices often access information that is considered sensitive for example banking details stored in messages, calendars and personal schedules, photographs, documents retrieved from emails, various social media platforms among other potentially sensitive data makes these devices targets for various individuals seeking to acquire such information for malicious purposes. This has led to the development of various security features to ensure safeguard of information on devices running Android operating systems (Shabtai et al, 2010). The outcome is a more secure device and ease of decision making on the part of the device regarding various issues associated with security. Android devices offer features such as the Android Application Sandbox developed to separate application data from execution by other applications present in a device, cryptography to safeguard information through encryption, a series of permission acceptance mechanisms including access control using passwords, voice, and facial recognition, memory management using technologies like ASLR and NX, encryption and deletion options to safeguard data where devices are lost, and application control for individual applications on mobile devices ("Filesystem Encryption").

2 Security Areas

One of the most important security areas is the integrity of data and information stored on the device running Android as an operating system. This makes data storage an area of concern for users. Third party service providers normally save on the Android system's internal device storage memory, external storage memory, or on the cloud data. Accessibility of data stored in various ways on the mobile device is an area of concern especially where applications on the device are able to access the said information. The idea is to ensure that information stored on the internal mobile device storage is accessible to authorized applications only thereby providing some form of security for the device ("Android Security Overview"). Malicious applications for instance run malicious code on devices allowing them to access information stored on the

device without the authorization or knowledge of the user and transmitting the same to predetermined destinations. By default, data stored in the internal storage is only accessible to the authorized applications ensuring some form of security from access by third parties. Ensuring that unauthorized applications do not gain access to this data is important with this done using encryption of files using keys not accessible to applications.

External storage provides additional space for data storage on Android based devices. This is done by use of memory cards that are unfortunately accessible to third parties allowing for both read and write capabilities ("Android Security Overview"). It is also possible to have applications access, and even modify this data making loss of the same relatively easy. The first step towards protection of information is avoiding storage of useful personal data on external storage ("Android Security Overview"). The fact that applications can access this data further presents an increased likelihood that data stored together with executable applications in memory cards is vulnerable to both loss and execution allowing for access by third parties. It is important to ensure validation of information accessed by the device from external storage prior to use by the mobile device ("Android Security Overview"). External storage service providers on the other hand allow users to store any type of information on secure clouds. The content is accessible using applications selected by users. Therefore, it is imperative that one allows access only to specific applications trusted by the user.

The other area of security is permission usage. Applications on devices running Android as the operating system are sandboxed to avoid interaction with each other without permission. Ensuring that applications have minimum permission requests is a way of safeguarding information stored on devices ("Android Security Overview"). Communication, which is one of the uses of mobile devices, presents another security concern. This is especially the case where data transmission takes place using the wireless connection option offered by most Android devices. Safety using the internet is important in various applications as it is possible to gain access to devices using this channel. Telephony further presents a risk especially where text messages are used ("Security Tips"). Interception of messages is possible. Therefore, it is necessary to remain cautious when accessing unauthenticated messages.

The popularity of Android as a mobile operating system makes it a popular target for hackers who rely on malicious applications to harm users. The fact that Android allows users to install software into devices without screening the same for integrity presents a security risk to users who install applications without adequate information on the same. This is the reason why Android, unlike iOs from Apple, accounts for up to 79 % of malware in mobile devices (Gilbert, 2013). Mobile operating systems like iOs are more secure than Android mainly because of the ability to push essential security updates to all devices. End users mainly because of service provider or hardware manufacturer do not always receive android updates thus the potential for security breach and exposure of user data to the risk of loss (Gilbert, 2013).

3 Areas of Security Addressed

Areas of security addressed by this topic include cryptography, data storage and retrieval, permission usage by various applications, network based security, and security provided by applications that seek to identify malicious code and executions within the device. While it is impossible to eliminate all potential areas of security breach, it is possible to minimize the risk of access to the same by third parties by taking precautionary measures such as ensuring that sensitive information is not stored on mobile devices, using strong passwords, and allowing execution permissions to trusted applications. The fact that individuals are using mobile devices as replacements for the personal computer presents an increased risk of information loss where devices are lost, intercepted by third parties on networks, or accessed by applications and through networks. The Android operating system is not foolproof therefore ensuring that access to devices by third parties is limited and that safeguards are in place to avoid potential interception is central in ensuring device and content security (Enck, Ongtang, McDaniel, 2009).

4 Recommendations and Conclusion

The acceptance of smartphones and tablets has led to the rapid adoption of these mobile devices and consequently introduced the risk and possibility of data loss from the same. Many device manufacturers develop hardware that runs on the Android operating systems. Some of the low end-product manufacturers have opted to leave essential security features when developing leaving holes that malicious individuals and applications can use to access information stored on devices. Users of Android devices ought to remain cautious when purchasing mobile devices and consequently ensuring they purchase devices from reputable manufacturers. This eliminates the risk of loopholes such as hardware flaws allowing application developers to exploit the same to gain access to device contents. Using tools to ensure security of devices for example encryption, use of strong keys, use of antivirus and antimalware applications from reputable developers, avoiding storage of sensitive data on devices, and ensuring that communication over networks is safe for example when accessing the internet

can easily provide security for information stored on devices ("Security Tips"). Google, the proprietors of the open source Android operating system should further ensure that applications provided on the Android marketplace are safe and free of malicious code. This has for instance happened with the Apple application development teams. The operating system requires improvement and more provision of advanced cryptography features to ensure safety for users. Google should also ensure that device manufacturers meet strict quality tests when it comes to product development to eliminate flaws in hardware security.

REFERENCES

[1] *Android Security Overview*. Retrieved from http://source.android.com/devices/tech/security/index.html
[2] Gilbert, D. (2013). *Google Admits Android Security Problem- But it May Never be Fixed.* Retrieved from http://www.ibtimes.co.uk/google-admits-android-security-problem- random-number-499319
[3] *Filesystem Encryption*. Retrieved from http://source.android.com/devices/tech/security/#filesystem-encryption
[4] *Security Tips*. Retrieved from http://developer.android.com/training/articles/security-tips.html
[5] Willems, E. (2013). Android Under Attack. *Computer Fraud & Security*, 13-15.