IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Review and Enhancement of security in Mobile Computing Devices

Shubham Dwivedi[1], Akanksha Deep[2]

School of Computer Engineering, KIIT University, Bhubaneswar, India[1,2]

Abstract: One of the fastest growing technology of today's world is mobile computing. It is growing at an exponential rate. Most of the complex tasks which required computers can now be done using mobile devices like smartphones at the touch of a finger.Out of all the mobile computing devices, the smartphones are most popular. The smartphones have now become an integral part of our lifestyles. Though the Smartphones help to increase the productivity, they also pose an underlying serious security threat. This research paper aims to review these potential threats, state the efficient methods to tackle them and draw conclusions for further research opportunities in this area.

Keywords: Mobile devices, Smartphones, Attacks, Security

1. INTRODUCTION

Mobile computing refers to the ability to use computing capabilities on devices which are not location specific. These devices are portable and can be used on the go away from their workstations unlike the traditional computers. Their functionality is not limited by their location. Thus, absence of these location specific constraints allows the users to request, retrieve and change information from anywhere. The basic principles of mobile computing include portability, connectivity.

All these features have led to a widespread use of mobile devices. Mobile devices include personal digital assistant(PDA), tablets, smartphones etc. Out of all these, Smartphones are most preferred choice. Mainly because of their small size and high computational power.Smartphones are playing a major role in business as well as our social lives. They are used to store personal as well as organizational data and therefore have become a source of risks. There has been a rise in the reports of vulnerabilities and attacks on the smartphone. These vulnerabilities compromise the safety of otherwise productive devices.

We have addressed the security issues in mobile computing by reviewing vulnerabilities and threats in the most commonly used mobile computing devices, smartphones and have also provided various counter measures to efficiently secure the devices. This paper is organised as follows, section 1 briefs about the smartphones, section 2 mentions the sources of attacks, section 3 details are givensome of attacks and the section 4 is about the security solutions to mitigate and tackle the threats.

2. SOURCES OF ATTACK

2.1. Internet- Internet is one of the main sources of attacks on the smartphones. Smartphones are connected to the network through Wi-Fi and mobile data. If the network is compromised, the security of the devices is at risk. Hacking of user data and spreading of viruses and malwares is possible through internet. This can be through mails and messages, which contain the link to the virus files. PINs, passwords and banking details can be stolen over the internet. It can also be used to send malicious spam mails. Also, there is a possibility of someone doing unlawful act under the access point name of others.

2.2. Applications - This is also a major source of attacks in smartphones. With the increase in demands of apps, there are also many fake apps with the sole purposes of stealing or destroying user data. They usually disguise themselves as genuine applications but once the user installs them, they gain access to software and hardware, which can now be modified by the application. They can steal the information as well as modify the stored information.

2.3. Desktop computers- Smartphones have a chance of getting infected by a virus or a malicious program, if they are used in synchronisation with a desktop computer which contains viruses. Although the number of such PC viruses which can affect the mobile devices as well is less but there is a risk of phone's storage getting corrupted.

2.4. Bluetooth- Devices with Bluetooth connections possess a risk of receiving as well as spreading viruses and worms over the Bluetooth connection. For example, one of the first smartphone worm to be detected, Cabir, used Bluetooth connection to find and spread to the nearby devices. Also, some applications allow the user to access and control other's devices if they are connected over Bluetooth.

2.5. Hardware- hardware attacks are generally referred to as low level attacks but can be triggered by malwares. They lead to the phone's hardware getting compromised. Camera, storage, sound etc. can be affected. For example, they can gain control of the camera and click user's pictures without consent.

DOI 10.17148/IJARCCE.2016.56114

3. TYPES OF ATTACKS

There are various types of attacks on mobile devices. Some of them are Sms based attacks - in this a phone gets infected through sms. This can cause the phone to malfunction and also infect other phones by sending sms/mms automatically. Wi-Fi based attacks – Smartphone user's data such as passwords can be stolen by the hackers over an unsecured network. Web based attacks – Such type of attacks is very popular and widespread. These include phishing pages, unsecured, fake plugins and websites which can lure the user into believing them to be authentic. If the User, uses these, his personal credentials are available with the creators of these pages, who can misuse it.Viruses and malware – if infected programs such as viruses and malwares get into the system, they can affect the corrupt the device. They can steal modify and delete the data.

4. SECURITY SOLUTIONS AGAINST THE ATTACKS TO SECURE THE DEVICE

As we have seen, there are numerous attacks which put the device at high risk, lead to data loss, data integrity threats and also resource abuse. They make the device a source of problems, which, otherwise is a productive tool. Thus, the devices need to be secured to as much extent as possible. For this we have to select the most suitable option from all the available solutions and implement them either individually or in combination.

In this section we have presented various security solutions, at different levels and also mentioned the different aspects of mobile devices in which they can be applied.

4.1Securing the hardware

Securing the device hardware is the security at the primary level. Modifying the hardware and making them more secure, will drastically reduce the chances of it getting compromised. It makes the smartphones less vulnerable to the attacks. For example, the sim and memory chip information can be encrypted. Also, the latest hardware should be used to make the device. Only the genuine and trusted hardware should be used. Nowadays, smartphones come equipped with finger print scanner. Only the user who's finger print is registered is able to unlock the device. This feature secures the device to a great extent as only the authorized person can use the device. All such security measures to secure the hardware ensures that the Smartphones cannot be easily tempered with

4.2 Securing the software

Another most common security solution for mobile devices is, securing the software of the devices. This can be done in two ways. One way is to improve the security of the operating system and the other way is through the third party applications such as antivirus. Smartphones run on operating system, which acts as an interface between the application and the hardware. Application access and control the hardware through the operating system. Operating system can decide and limit the resources available to the applications. It can restrict the harmful applications to use the hardware, thus saving from potential threats. For example, some malware automatically connects to internet and some of them can click photos without user's consent. Operating system can stop this by limiting the application permissions. Another way is by installing third party apps such as antivirus to detect and prevent the harmful files from affecting the system. Antitheft application can be used to prevent data leak in case of theft and also to locate the device. Rootkit detector systems can also be used to detect the intrusion of rootkits. All these measures at the software level can greatly secure the device and ensure its smooth running.

4.3Securing the network

Almost all the smartphones are connected to network for exchanging and accessing information. This can include wide range of services such as making calls, sending and receiving sms and connecting to internet. It is also one of the sources from which many attacks find their way to the devices. Internet network is a major source of attacks and threats. Thus needs to be secured. One of the steps, which can be implemented by the internet service providers is to ensure that all they devices in their network are verified and trusted. That they have the latest security patches and follow the set security guidelines. Also, the network traffic exchanged by the devices should be monitored. If any abnormal behaviour is detected, it should be stopped then and there. There should a highly secured and strict set of protocols for the exchange of data between the devices.

The data which is exchanged and stored should be encrypted. Also, the telecommunication providers must ensure to provide filter for spams.

5. CONCLUSION

In this paper, we reviewed the security of the most popular mobile computing device, the smartphones. We briefed about why it is necessary to emphasize on its security and make it intrusion free. We stated various sources from which threats are possible. We also examined various kinds of attacks and how they get executed. We saw how the attacks find their way into the target system. We analysed the consequences of these attacks, that is how and to what extent they can affect the device and the user. Finally, we mentioned various solutions, which can be implemented at both personal and organisational level to improve the security of the phones and make them more secure. The matter presented in this paper can also be used as reference for further research in the field of mobile device's security.

REFERENCES

1. M. Kotadia, “Major smartphone worm by 2007”
2. N. Leavitt, “Malicious Code Moves to Mobile Devices”
3. https://www.computer.org/
4. https://securelist.com/
5. http://www.scmagazine.com/mobile-security/topic/9541/
6. http://antivirus.about.com

DOI 10.17148/IJARCCE.2016.56114