



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 4 , April 2017

Methods to Hack and Secure mobile Data

Ms. Sangeeta Garg , Ms. Aeshwarya , Ms. Suman Kumari

Assistant Professor, Computer Science Department, K.L.Mehta Dayanand College for Women, Faridabad, MDU, India
Student, M. SC., K.L.Mehta Dayanand College for Women, Faridabad, Haryana, India
Student, M. SC. , K.L.Mehta Dayanand College for Women, Faridabad, Haryana, India

ABSTRACT: With the advent of technology, the use of android phones is also increasing. Today's Android devices make us feel that our wallet is in our pocket. These contains our personal information and it become necessary to secure this information. With the increase in technology many security issues are also increasing. In this paper we have explained the major threats to mobile devices and have used one of them as a methodology to show how it works. Also we have used a method to secure our devices using apps.

KEYWORDS: vulnerabilities, apps, security, mobile device

I. INTRODUCTION

Recent developments in the field of mobile phones have made our life easier then ever before. Mobile has become a cornerstone of the global economy; use of mobile applications continues to rapidly[1]. With the advent of digital era, mobiles are not limited to just calling, receiving, and texting. Instead of this, today phones support many features such as taking pictures, online payments, communications, sharing documents, business purposes, etc. All of this is possible only due to upgraded technology. We can say mobile phones today has become smart. So we possesses banks, business, booking in hotels, restaurants, shopping, etc in our hand only in a small device we call our smart phone.

A. What is a smart phone?

We can define a smart phone as a mobile device having a touch screen, internet access and an operating system capable of running various apps. These smart phones works same as desktop workstations in terms of storage and installing numerous applications.

We can define a smart mobile as below

MNO(Mobile Network operator)+ Mobile device= Smart Mobile [2]

II.MOBILE THREATS

There are four types of threats to mobile devices. They are as follows: [3]

- 1 Application based Eg. Malware
- 2 Web based Eg. Phishing
- 3 Network based Eg. Wifi sniffing
- 4 Physical threats eg. Bluetooth

A. What are apps?

Mobile phone apps are programs of small size made for phones. These are helpful in business today. Some other advantages of apps can be :

- Easy access through gadgets
- Introduce sedevices to international market
- No restrictions for the owner



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 4 , April 2017

- Does not depend on the specifications of smart phone
- Good customer communication
- Entertainment
- Sharing of documents
- Educational help
- Online payments

Example : Amazon, WhatsApp, pay tm, games, talking tom, etc.

III. SECURITY CHALLENGES

Security can be defined as the capability of software to prevent deliberate or inadvertent unauthorized access to code or data[4]. Authenticity, confidentiality, integrity accountability and availability are some of the security aspects[4].

Now-a-days, smart phones are the fastest growing technology and gaining more and more consumers each day. Diverse data is transferred and exchanged on this platform only. Applications like banking, e-commerce, internet access, medical usage, entertainment, remote working on these smart devices. But some people still think before using this smart device and sharing their personal data to them. The reason is its security issues. So it is important to secure smart phones to use them without any hesitation and keeping data safe.

Some of the security challenges can be as follows : [3]

- 1 Poor authentication
- 2 Insecure data storage
- 3 Security decisions via un-trusted inputs
- 4 Sensitive information disclosure
- 5 Broken cryptography
- 6 Insufficient Transport Layer Protection
- 7 Server side controls
- 8 Client side injection
- 9 Side channel data leakage

IV. VULNERABILITIES TO MOBILE DEVICES

Mobile phone security has become a hot topic these days. Users have their personal data which they want to be safe from any one else. Many business also rely on smart phones. Any vulnerability can cause a serious damage due to loss, theft or alteration in their data. Data could also be mis used.

Few vulnerabilities to the mobile devices can be : [3]

- Trojan horse
- Botnet
- Worm
- Root kit
- Phone as microphone
- Various apps

Any Android phone can not initiate or end call on its own without the user's permission. But a feature was introduced in 2008 which can do this without the user's permission with the malware[5]. Using this hackers could easily lock sim card, delete data on your phone or interfere with normal calls due to this vulnerability. Also hackers could affect you by making same phone as your using cloning technique.



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 4 , April 2017

Technical security measures are uncommon on mobile phones. Any vulnerability to these measures such as firewalls, antivirus and encryption can provide an entry for attackers. Hackers can compromise your mobile phone, listen to your conversation without you being known about it. As per the info provided by some benchmarked authorities, from 2009 to 2010, the no. Of new vulnerabilities in mobile OS has jumped to 50% [6].

V. METHODOLOGY

In this paper we have used the method based on application threats. How a phone can be hacked and secured is presented below :

How it is hacked?

- 1 Start.
- 2 Take the victim's phone. Download the application " Copy9-phone spy" or "Copy9".
- 3 It needs some settings to be done. Go to settings. Click on security on the unknown source button.
- 4 Now open the application. Click on register. Create your account using email & password.
- 5 After registering, hide the app.
- 6 Then clear browse history from victim's phone.
- 7 In your phone, go to Google and type login-copy9.
- 8 Now enter email and password which you gave in the victim's phone. You will get all the information of victim's phone.
- 9 End.

This method of hacking could also be performed using various other apps such as Spy human, Android play store, the truth spy.

How do we know our phone is hacked and how to secure our mobile device?

- 1 Start.
- 2 Download "AVG antivirus free for Android".
- 3 Open the app and click "scan".
- 4 If your device is safe, it will show " successfull, there is no malware".
- 5 If there is malware, it shows the malware attack on our mobile phone.
- 6 Then, it will ask to remove that. Click "remove". Now our phone is safe.
- 7 End.

The above method of scanning and removing could also be performed using other apps such as free spyware and malware removal, anti spy mobile, kaspersky antivirus.

VI. PROTECTIVE MEASURES TO BE TAKEN

Mobile phones can be hacked using various apps today. There are no. Of apps which access our personal information because we don't pay a little bit of our attention while downloading those apps. Suppose we download any game then can we think for a while that why would it need access to our contacts? So be careful while accepting the permissions of apps in your phones.

Some of the steps to protect can be :

- Check security features during choosing mobile devices
- Organise the device to be more secure
- Configure web accounts
- Do not click links sent in emails or text messages
- Revelation of mobile phone no. On social networking websites



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 4 , April 2017

- Think before you store personal information
- Choose correct apps
- Vet your apps. Make sure about ratings and comments. Always read the permissions before clicking "accept".
- Disable interfaces when not in use such as Bluetooth, wifi, infrared
- Do not root the device
- Don't leave your phone lying around for others

VII. FUTURE SCOPE

With the advancement of technology, vulnerabilities are also increasing and solutions are moving towards being biometric. Data security is the topic of concern in today's digital era. It is a hot topic for research and future development. Mobile phone security is more than just protecting your device. It is a key to one's digital identity now.

VIII. CONCLUSION

With the increased in the digital era, many malicious people also try to break the security to access the data and to complete their actions which they want to do such as alter data, harm or misuse of the data. There can be two types of attacks on the mobile phones. One, when the phone is connected to the network. Secondly, when it is connected to the internet. Increasing no. Of vulnerabilities and security issues has risen the need for biometric solutions as there is no clear solution.

REFERENCES

- [1] State of mobile app Security, apps under attack, research report/ special focus on financial, retail merchant and healthcare/ medical apps
- [2] Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices, Michael Never, felix. C freiling Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Woff, 2011 IEEE
- [3] "mobile device security: survey on mobile device threats, vulnerabilities and their defensive mechanism" sujithra M, Padmavathi. G
- [4] Mobile application security platforms survey, January 2016
- [5]Google
- [6] www.forensicsware.com.