ISBN No.: 978-81-941751-0-0

PAPER 12

MOBILE APPLICATIONS SECURITY: AN OVERVIEW AND CURRENT TREND

P. K. Paul[1], P. S. Aithal[2]
[1]Executive Director, MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India
[2]Vice Chancellor, Srinivas University, Karnataka, India
Corresponding Author: pkpaul.infotech@gmail.com

Abstract

Mobile Security is an emerging concept and name in Information Technology Security. It is very close with Mobile Computing and concerns with the securing mobile based services and products. It is the protection and system against the attack and vulnerabilities and applicable to the smart phones, tablets, laptop etc. Mobile Security is also related with the wireless security. The concept of securing mobile devises becomes important and valuable and increasing rapidly in recent past. Today the organizations and institutions of different kinds are using various Information Technology tools and components and all are connected to the internet or online systems and as a result vulnerability became crucial. The mobile applications security may be two types active and passive. The device loss becomes an important concern and apart from these few important are application security, device leakages, malware attack, device theft etc. The individuals are also employing different tools and devices and all such products become challenge now days. There are different methods in attacking the systems and also preventing. All these attacking systems and preventing systems are increasing day by day. The domain Information Assurance, as deals with both technology and managerial affairs of the security; so the Mobile Security field is also an important area of the field. This is a conceptual paper and theoretical in nature and deals with several affairs of Mobile Security.

Keywords: Mobile Security, IT Security, Cloud Security, Information Assurance, IT Protection, Digitalization, Information Systems

1.Introduction

Mobile Security is the need of hour; organizations, institutions and individuals are today actively engaged with the mobile and similar devices and all such devices are great threats due to many reasons. Mobile Security or mobile device securities etc are today an important concern of Information Security [1], [5]. There are different means for the attack and its prevention and among the threat of attack few important attack zones and areas are SMS and MMS, in Telecommunication Systems, attack based on GSM and Wi-Fi, Bluetooth systems, web browser, operating systems, attack based on hardware and infrastructure, password cracking in secured software, malware etc [2], [3].

ISBN No.: 978-81-941751-0-0

There are different reasons for the security and among these device loss are important concern, many a times we may forgot to take the devices or simply lost the devices [4], [8], [9]. Application security is another concern, which is also very important to take. Today many applications are available freely and that comes with different features and all these vulnerable in many contexts. Similarly data leakage is another concern and data loss results the malicious attack in some cases Malware attack is another concern that concerns about the Mobile Security. According to a study it has been noted that 81% of mobile malware are Trojans, and then rest it monitoring tools (10.1%) and also few malicious applications (5.1%). Today each and every organizations are giving importance to the wireless and mobile security there are different measures available to solve these, and different organizations are also involved into this [5], [6], [7].

2.Objective and Agenda

As the current paper is theoretical and conceptual in nature and thus deals with various affairs leading to Mobile Security and allied areas and among these few important are—

- To learn about the basics of Mobile Security including its features, characteristics and nature.
- To learn about the field of Mobile Security and allied areas in brief.
- To find out the threats and attacking systems to the mobile based IT products and services in brief.
- To learn about the basics of prevention methods of Mobile Security in simple sense.
- To learn about the limitations of such security measure in brief.
- To learn about the Mobile Security Management concepts and tools to manage the overall system.

3.Mobile Security: The Root

Mobile Security is very much close with the wireless security. Very simply, Mobile Security is nothing but the securing mobile services and mobile devices from the third party attack or vulnerability. Today profit making as well as nonprofit making institutes are engaged with different kind of tools and technologies and most of these are mobile based and thus Mobile Security is very close concern about this [6], [10], [11]. It is worthy to note that previous to the concept of Mobile Security the concept of computer security got popularized which is small area and very close to securing the computer itself. Gradually other areas of security has been conceptualized and among these important are IT Security, Information Security are important.

IT Security is concern with different sub fields viz. Web Security, Network Security, Database Security and so emerging areas viz. Cloud Security, Mobile Security etc. Hence Mobile Security is the part of advanced IT Security in many contexts. Different Companies are using different strategies for the Mobile Security and among these, one important is allowing client and employers to use only respective or selected devices only. It has been noted as per a latest survey that 84 % of the threats are fall under the Trojans and rest from other insecure systems. Thus most of the organizations and institutions are using Mobile Security tools and strategy to keep the system smart and advanced [6], [12], [14].

The field Mobile Security is very close with the Wireless Security as well. But wireless security concept developed earlier than Mobile Security and today apart from wireless

ISBN No.: 978-81-941751-0-0

security it is very much close with the cloud security, mobile computing as well [11], [13], [15].

4.Mobile Security and Attacks or Threat

Mobile security is an important part of today's Information Technology world. It is very close with mobile computing. In other word it is also called as security of mobile based devices like smart phones. Mobile security normally associated with smart phone, computer etc by the attackers. Normally this comes with short message service (SMS), multimedia messaging service (MMS), WIFI, Bluetooth etc. However few experts are also warns about the operating system security because attackers may use different objects by the browsers or OS or malicious software's. It is worthy to note that downloadable apps sometime also cause for mobile security. Any smart phone or electronic devices should come with privacy and integrity applications. According to network expert the major target of the attackers are-

Data: As smart phone or electronic devices contains different kind of sensitive or virtual information such as –credit card no., authentication indication, audio, visual content, call log etc. So this is the prime target.

Identity: With an electronic device the owner can be indentified easily and hare attackers may use this identity for different purposes.

As far as modern threads are concern with mobile security; concerned with different objects such as-

1. Boot nets
2. Spyware
3. Malicious link
4. Malicious applications

The first one normally holds malware and user get it normally by email attachment. Boot net is a combination of robot and network and it is normally denoting malicious affairs. Here attackers from the network place can control the device and harm the overall system.

Spyware is useful simply to highjack the phone including hare the calls, see the text and content, to know the location of the device by the GPS.

Malicious link normally spread on social networking site for wider distribution and that can be by the backdoors.

Malicious application is available in different app platform. It is useful to get personal information or to enter into the system.

Most of these attackers belong to different community. Many of them are unethical hackers, some of them are professional and they may work in commercial house or military services. However the concept of black hat attackers and grey hat attackers are gaining popularity.

5.Different methods in Mobile Security

There is different attacking system for mobile security and that may cause in the following-

1. Attack based on SMS and MMS

ISBN No.: 978-81-941751-0-0

2. Attack based on different kind of network like GSM network and WIFI based network
3. Web browser
4. Operating system
5. Hardware and vulnerabilities
6. Insecure software etc.

In mobile security **SMS** is also a weak point sometime. It causes in the mobile system having binary SMS system. It leads the denial of service attack. We can see such witness in SIMENS S55 model having Chinese Character. Similarly in earlier days few Nokia phones are also unable to recognize denial of service attack. It is important to note that distributed denial of service is also an important attack to the mobile and the telecommunication system.

In mobile security another focus attacking place is **GSM** network. The GSM encryption belongs to **A5** algorithm and their vulnerabilities is an important concern. We can see this kind of attack in some of the Europeans countries. Gradually **A5/3** and **A5/4** algorithm have been popular against this kind of attack. After the development of 2G GSM we can see the vulnerabilities. The hackers in recent past can also break the GSM algorithm.

As far as the **WIFI** is concerned in recent past the attackers can get information of a smart phone by find out the vulnerabilities. The security of wireless network previously secured by **WEP** (Wired equivalent privacy algorithm) keys but the weakness of WEP altered by WIFI Protected Access **(WPA)** and **WPA3** algorithm. The protocol Temporal Key Integrity (TKIP) has been introduced to allow the migration of **WPA2** and **WPA3**.

In the recent past security is also an important concern for **Bluetooth** system. With Bluetooth one can easily break the vulnerabilities. The attackers are required to connect to port for accessing or controlling the device or mobile. In Bluetooth system attackers send a file and if users download the file then the system may be corrupted such as CABIR (SYMBIAN).

6.Security Management & Mobile Security

There are different tools and defending methods exists for Security Management and among these few important are as follows—

Operating Systems—

Operating System is the core of Mobile devices and there are different mechanism for ensuring and protecting Operating Systems from the threat. Smart phones are able in accommodating different kind of applications into it and thus there should be proper mechanism to detect the vulnerabilities and any kind of virus, malware, spyware etc. Sandbox is an important matter in mobile and each mobile phone needs to plan for specific Sandbox in this regard. Few important concern (mainly in Android) in this regard are include—

- The intrusion of the rootkit is very important and thus proper rootkit detection mechanism is very important.
- Process isolation is also very important in android based systems and for proper and scientific security this should be keep in mind. Moreover here each process once start should complete and then only may enter other program. This approach will reduce the chances of vulnerability.

ISBN No.: 978-81-941751-0-0

- File system permission is very important concern of android based systems and use of locking memory permission is also with this kind of system.
- Memory protection is an important feature and function of Operating Systems of android based or any similar kind of devices.
- Development through runtime environment is an important concern and here valuable to note that high level language based designed products are suitable for this purpose [7],[16], [18].

Hardware Systems—

The hardware system is vulnerable in different situations. There are different types of attacks/ vulnerabilities viz.—

- Electromagnetic waveform is a vital reason for the attacks and these are increasing every day.
- Juice jacking is the vulnerability of mobile security in different context. This is may be applicable in public places during charging of mobile phones in the bus, flights, train and other places. Such type of incident may noticed in different places. Different malicious attacks may be happen in this case. Here actually, USB charger mainly used for the attacking victims.
- Jail breaking and rooting is another vulnerability and related to the physical vulnerability. It is related to the operating systems security.

Malicious Software based Vulnerability—

There are different types of vulnerability can be noted in malicious software as far as Mobile devices are concerned. These days smart phones are highly using for the internet purpose and we aware that a malware is a program responsible for harming the system. A study noted that, the malware variant has been increased in recent past up to 54%. Worms, viruses are considered important in this category [17], [19]. The malicious attacks can be possible with three types viz.—

- Infection of the systems and that can be classified into Explicit Permission, Implied Permission, Common Interaction, No Interaction—all these malicious software are important to attack the mobile device.
- The accomplishment of its goal; which include the affecting the systems after entering the malicious software into the systems and that is done by the monetary damage, damage data and/or device, as well as concealed damage.
- Spread of the malware to other systems is another way to vulnerable the systems and among these important. Here Wi-Fi, Bluetooth and infrared or even using remote networks viz. telephones calls or SMS or emails spreading can be done.

Day by day the malware is increasing and these include the Viruses and Trojans, Ransomware, Spyware etc. Though, according to the Information Scientist few attacks of the systems are includes (refer Fig: 1)

ISBN No.: 978-81-941751-0-0

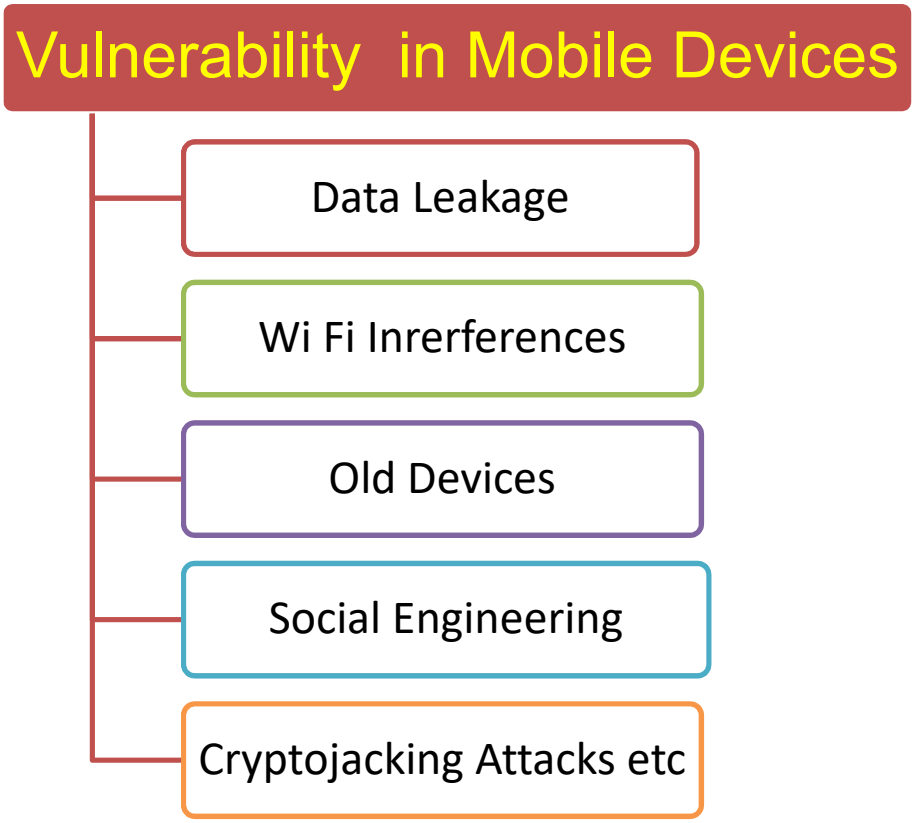

Fig: 1- The vulnerability in Mobile Devices at a glance

7.Mobile Security Policy and Countermeasure

The Mobile Security can be bring with different countermeasure and policy and among these few important are include as follows—

In Operating Systems—

In a mobile, the first preference of the security is required for Operating Systems; resource management, schedule processing and other components role needs to be useful and secure in different sense. The sandbox is the important component of the mobile; where different applications are stored together and thus it is required the operating systems should be secure.

In Security Software—

Security Software is another important component and way to secure the mobile devices. Apart and above of the operating systems security this is important and essential and this is required to protect the mobile systems. Antivirus and firewall is essential to protect the systems. Importantly, it is required as signature detection software detects malicious executable files. The following are important concern in this regard—

- Visual Notification is another important action required for securing mobile devices; especially mobile phones. This is the image based result, viz. incoming call

ISBN No.: 978-81-941751-0-0

information on the display unit. Hence if a call trigged by malicious apps that can be noted and detect, if possible.

- Turing Test is another way to bring the security in the mobile devices. It is the applications of Artificial Intelligence; required to distinguish human and virtual users; viz. Captcha.
- Technique of identifying a person by means of their morphology is another security measure. The field in generally may be called as Biometrics. Biometrics is used by studying face, eyes etc. Here no need to remember the password as well. Hence this can be a good tool for mobile security.

Resource Monitoring in Devices—

There are different ways in resource monitoring and we can get an idea on suspicious attack and among these few important are depicted as follows—

- Monitoring battery consumption of the phone may be useful to detect whether any malicious application running or not.
- Every application has a specified memory requirement and it can be suspicious when a applications requires more than that.
- In smart phones many applications are run via network and *like previous point on memory*, the speed of operation of the application can be monitored. Sometimes higher bandwidth than the requirement can be treated as suspicious.

Network Related Issues—

As far as Network Surveillances is concerned following are important to noted—

- Spam is common in Emails and thus for the Emailing services in mobile spam matter should be consider as important.
- Encryption of stored information and data needs to be keep safe and here encryption may be used. Additionally for transferring data also encryption algorithm can be useful.
- Telecom Network monitoring is also important issues for secure mobile based services.

Product Development and Manufacturing—

As far as product development and manufacturing is concerned few things are important and among these valuable are—

- Deleting debug mode is very important in the mobile phones. This mode needs to removed in the devices before its sell to the consumer. Today one manufacturer developed lot of devices and sometimes they sold it in debug mode; so these should be keep in mind carefully.
- During the selling of a smart phone it is essential to keep that in Default setting; otherwise that can led Denial of Service attack.
- The smart phone market is emerging and with lots of applications. It is worthy to note that the security audits of applications are very important and valuable otherwise the whole system may be corrupted or infected.

ISBN No.: 978-81-941751-0-0

- Every applications in the android system is asked for permission during its installation and thus during such activity it is essential to read the content carefully and if found unethical or suspicious information.
- Revocation procedure is another one in android system and can be managed by the app provider or system administrator; here uninstall of the app is possible globally. Hence this way security can be ensured.
- Avoid heavily customized systems, may have dual effect of risking the introduction of new bugs in the system and it is an important security concern.
- The updates of the software or patches must be come with the documentation by the manufacturer. Hence by reading everything one can update the systems easily.

User Awareness—

User awareness is very important for running safe and secure android based system. It is a fact that most of the users are not read carefully the messages and details of the applications. Here application provider reputation, security messages, agreement messages are very important. Even there may be some software or application with intensions of phishing etc. Caring the phone with the owner is also important security measure in some cases. Different organizations and association has provided different framework and guidelines all of these need to follow by different stakeholders (refer fig: 2 for details). Different apps and system need to closedown if not required viz.—

- Digital camera
- GPS
- Bluetooth interface
- USB interface
- Removable storage etc.

Moreover latest android phones are come with inbuilt encryption systems with this it may be difficult to hack the systems or loose the information. Here the system may be encrypt or SD card etc.

Centralized Storage Systems—

Sometimes it is better to keep the data and all the text in the company server and storage systems instead of Third Party Company or even own mobile devices.

ISBN No.: 978-81-941751-0-0

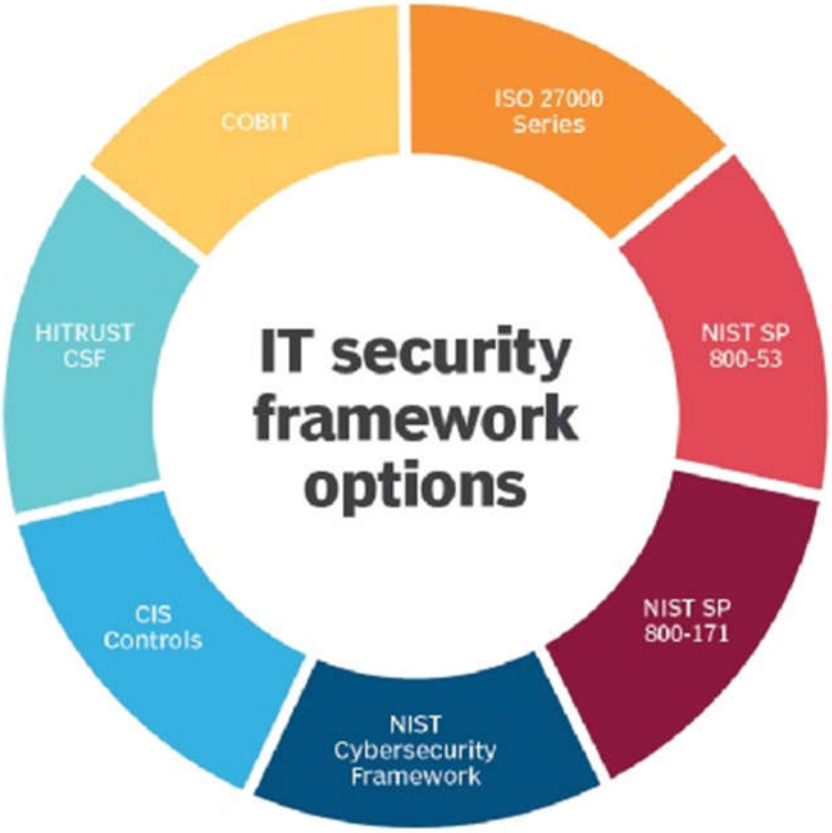

Fig: 2- Major IT Security Framework providers

8.Conclusion

As a whole Mobile Security is needs different counter measures and defending mechanism but still there are certain issues for which it is difficult to perform the security. And among these few important are Operating Systems. It is worthy to note that, few operating system are single tasking hence such are not capable to do the task along with firewall or antivirus. Energy autonomy is another important concern that should keep in mind. It is worthy to note that, network utilization should not be too high for the security reason. Apart from the technological countermeasure, it is essential to have users interest and awareness for the security related concern. Moreover, few things are essentials viz. rich operating systems, secure operating systems, secure element, secure applications etc.

References

[1] Bellavista, P., Corradi, A., & Stefanelli, C. (2001). Mobile agent middleware for mobile computing. *Computer*, *34*(3), 73-81.

[2] Bonner, W., & Chiasson, M. (2005). If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization*, *15*(4), 267-293.

[3] Borselius, N. (2002). Mobile agent security. *Electronics & Communication Engineering Journal*, *14*(5), 211-218.

ISBN No.: 978-81-941751-0-0

[4] Brooks, R. R. (2004). Mobile code paradigms and security issues. *IEEE Internet Computing*, *8*(3), 54-59.

[5] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications magazine*, *40*(10), 70-75.

[6] Djenouri, D., Khelladi, L., & Badache, N. (2005). Security issues of mobile ad hoc and sensor networks. In *IEEE Communications Surveys Tutorials* (Vol. 7, No. 4, pp. 2-28). IEEE Communications Society.

[7] Donald, A. C., Oli, S. A., & Arockiam, L. (2013). Mobile cloud security issues and challenges: A perspective. *International Journal of Engineering and Innovative Technology*, *3*(1), 401.

[8] Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017, May). Security and privacy issues for an IoT based smart home. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1292-1297). IEEE.

[9] Goth, G. (2012). Mobile security issues come to the forefront. *IEEE Internet Computing*, *16*(3), 7-9.

[10] Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional*, *14*(5), 28-33.

[11] Jansen, W. A. (2000). Countermeasures for mobile agent security. *Computer communications*, *23*(17), 1667-1676.

[12] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. *IEEE Wireless communications*, *14*(5), 85-91.

[13] Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: a review and recommendations. *Journal of medical systems*, *39*(1), 181.

[14] Ngai, E. W., & Gunasekaran, A. (2007). A review for mobile commerce research and applications. *Decision support systems*, *43*(1), 3-15.

[15] Nkosi, M. T., & Mekuria, F. (2010, November). Cloud computing for enhanced mobile health applications. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 629-633). IEEE.

[16] Siau, K., Lim, E. P., & Shen, Z. (2001). Mobile commerce: Promises, challenges and research agenda. *Journal of Database Management (JDM)*, *12*(3), 4-13.

[17] Siau, K., & Shen, Z. (2003). Mobile communications and mobile services. *International Journal of Mobile Communications*, *1*(1-2), 3-14.

[18] Siau, K., & Shen, Z. (2003). Mobile communications and mobile services. *International Journal of Mobile Communications*, *1*(1-2), 3-14

[19] Varshney, U., Vetter, R. J., & Kalakota, R. (2000). Mobile commerce: A new frontier. *Computer*, *33*(10), 32-38.