International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A LITERARY SURVEY ON SECURITY ISSUES ANDTHREATS IN MOBILE COMPUTING

Reshmi.R[1],Dr.G.Satyavathy[2]

[1]Research Scholar, Department of Computer Science, Sri Ramakrishna College of Arts and Science for women, Coimbatore

[2]Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science for women, Coimbatore

ABSTRACT

Mobile computing is a combination of mobile web and cloud computing which helps the mobile users to access applications and services on the internet. The goal of mobile computing is to enable high mobile application on mobile devices. The mobile computing is a process of computation on a mobile device. Nowadays, size of computing machines is being decreased with more power of computing, this leads to develop the concept of mobile computing like PDA, Laptop, cellphones, data storage devices and other mobile device. The security aspect brings most important role in mobile computing, it concerns the security of personal information and the other information of the users which is stored on smartphones. The usage of the mobile internet has changed the way where the users can reached the other users around the global instantly, from any resources over the internet. Security is a greater problem for wireless network, were radio signals are travel through the open atmosphere and they can intercepted by the individuals who are consistently on move and therefore difficult to track down. Security may provide a hardware approach to basic encryption and decryption capabilities. This approach is not applicable for all wireless resources. This paper deals with some of the threats that affect the mobile devices and also discuss about security issues, security techniques and requirements.

***Keywords*: mobile computing, security issues, security requirements, threats.**

I. INTRODUCTION

Mobile computing is a human –computer interaction, which allows for transmission of data, voice and video from where ever location that may be. This interaction helps to allow people to connect with the internet. The mobile computing device has some of the common forms which are portable computer, personal digital assistant/enterprise digital assistant, ultra-mobile PC, Laptop, smartphones and tablets, and wearable computers. The mobile computing has three aspects they are mobile communication, mobile hardware and mobile software. The mobile communication include ad-hoc network and infrastructure network and communication properties, protocols, data formats and concrete technologies. The other aspect is on the mobile hardware which is mobile devices or device components. The third aspect deals with the Mobile computing is taking a computer and all necessary files and software out into the field[1] . In the rapid growth in the wireless mobile communication technology, small devices like PDAs, laptops are able to communicate with the fixed wired network while in motion. Because of its flexibility and provision of providing ubiquitous infrastructure, the need to provide security increases to a great degree. In the case of mobility there is chance of theft of the information of the mobile users, the device is not shared by more than one user, only the network is shared. Due to this the sensitive information is hacked by the third-party.

II.MOBILITY AND SECURITY

Mobile computing is of a computing and communication were the devices are not restricted to a single place. In simple, mobile computing user can use the services of the internet while they are in movable state.

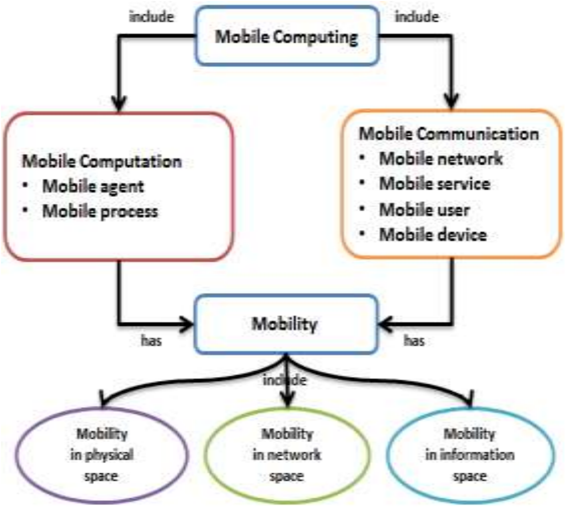

Fig1: Mobile computing

The set of security problems in mobile component in mobile computing is different to that in the traditional computing. The computer and database system is physically isolated from the other components in the environment by easily afforded by physical protection of fixed computing in traditional computing. In such configuration it was possible to make the system self-sufficient, without any need to communicate with the external world. More recent firewall techniques may also be applied to achieve the same effect. The isolation and self-sufficiency in mobile computing is hard to reach the relatively limited resources available to a mobile unit, so it communicate with the mobile support station. The users and the abstract that they carry a set of security problems from the existence and location of a user and the authenticity of information exchanged between users and a fixed host. The information of the user on mobile wireless network is treated as being confidential.

III. MOBILE COMPUTING THREATS

Mobile computing as variety of security threats which can affect the mobile devices. The mobile threats are as several categories that include,

- Application Based Threats
- Web Based Threats
- Network Threats
- Physical Threats

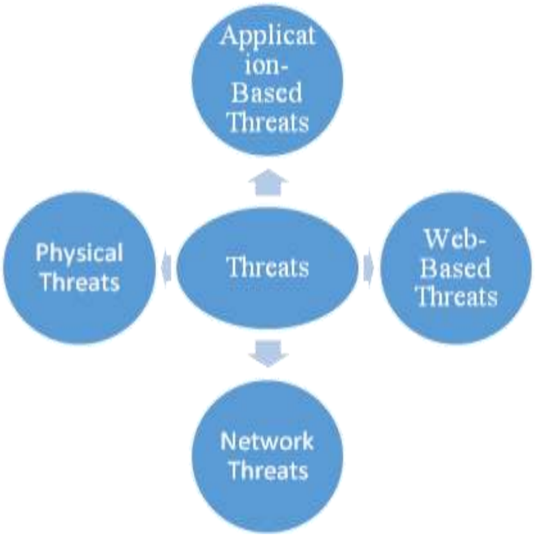

Fig2: Types of Threats in mobile computing

3.1 Application –Based Threats

The user when download an application from the website, some applications tend to be good on a website, but they are designed for commit a threats on the user mobile device. There are some application based threats they are,

3.1.1 Malware: Malware is a software which is designed for performing a malicious actions on user device, without the knowledge of the user. There are some types of malware which include,

- Virus: Virus is a program in a computer were it can create and install a copy of the files in the device, they can spread the files from computer to computer and they can do the changes in the files or they can stole the important data's in the files.[2]
- Worm: Worms as like virus they can replicate automatically and damage the multiple files, without the host file and without attaching an existing file. Worms instead of targeting single computer it damages entire network .Worms can access a computer through an email
- Trojan:Once a user enables them, they infect the computer. The Trojan is not self-replicating and can only be spread by user interaction, through email attachments or internet downloads.

3.1.2 Spyware

The spyware is used to collect or use data without your knowledge. Spyware target data includes phone call history, text messages, user location, browser history, contact list, email, and private photos. The spyware are as classified into adware, systemmonitors, cookies and Trojan.

Privacy Threats: The privacy threats is not malicious it collect or use the sensitive information such as location contact list and personally identifiable information.

Vulnerable Applications: The vulnerability allows an attacker to reduce the system information assurance.Vulnerability as three elements such as a system flaw, attacker access to the flaw, and attacker capability to exploit the flaw. The attacker access the sensitive information and perform malicious action, it starts downloading apps without your knowledge.

3.2Web-based Threats

Mobile devices are often connected with the internet and accessing the services in the web, that may lead to cause threats in the mobile devices. The web based threats are as various issues they are

Phishing: It attacks target company email websites, Gmail and popular sites like amazon. These websites are target for providing information such as passwords or account number. The attackers will create their own website like other websites (bank).The user may think that they are on the correct websites and they provide their password as requested. These leads to threats.

Download: The application can start download automatically when you visit a webpage

Browser exploits: When the user visits unsafe web page, user trigger browser exploit that can install malware or perform some actions on devices.

3.3 Network-Based Threats

Mobile devices typically support cellular networks as well as local wireless networks (WiFi, Bluetooth). Both of these types of networks can host different classes of threats:

- The network exploits as advantage of flaws in operating system or software that access local or cellular network. When the mobile is connected to the network then the malware is installed without the user knowledge.
- Wi-Fi Sniffing intercepts data as it is traveling through the air between the device and the WiFi access point. Many applications and web pages
- The user do not use proper security measures, sending data without applying encryption across the network then the data can read easily by the third-party.

3.4 Physical Threats

Mobile devices are carried anywhere at any time with us, so the physical security is also important aspect. The threat which leads to loss of data or physical damage to the hardware .The threats could be happened due to accidental or caused by natural disasters.

IV.SECURITY ISSUES

Mobile security has a key issue in mobile computing .The users use the mobile as communication tool for their services in the business. It relates the transmission of data over wireless networks. The sensitive information of users must be protected from the smartphones while they are on the network.

According Sonika [2] Dataloss from decommissioned device: if the mobile devices are lost or theft, the information of the devices is accessed easily by other user when the device as weak password, no password and no encryption. The threat of the data is high in this situations.

Data theft mobile malware : The android devices as option to download or installation from the third party sites instead of Google's official play store ,this leads to install the malware (i.e. malicious program which leads damage the device),without the user knowledge.

Data loss and data leakage: The mobile devices as application which has grown exponentially on android and iOS. These are mid-levelthreat. The data loss and data leakage is happened through the poorly written application across mobile operating system.

Vulnerabilities in the device: The mobile devices contains all the functionalities which provide the security concerns to hardware, os, and application developers. The possibilities of the threat is high, the number of exploits is not.

Unsecured Wi-Fi network access: when the mobile device is connected with the Wi-Fi connection then the device is in less security level the threat can happened at any time, the information can be able to hack by the third party.

Unsecured or rogue marketplaces: When the user attempts to install or download apps from the third party other than the Google's play store, it leads to distribute the malicious code for android device from the third party app stores.

4.1 Wireless security issues

The security issue which related of wireless networks which is intercepted of the radio signals by attacker, most of wireless network are accessed on other private network which is used by other users, this leads to less security procedures. The major security issues of mobile computing by using wireless networks are,

Denial of service (DOS) attack: It is a cyber-attack were the incoming traffic flooding which originates from several different sources. This is impossible to stop the attack service from single source.

Traffic analysis: The traffic flowing in wireless channel is considered by the user for identifying and monitoring the communication between users. The private information of the user can be accessed by the hacker.

Eavesdropping: When the wireless network is insecure and the data's are not encrypted then the hackers can be able to access the sensitive information of the user.

Man-in-the-middle-attack: The attacker's insert their host between the senders and receivers host, were the session intercepted and the transmitted information is modified by attackers.

Disconnection: The mobile user access the service of the internet at anywhere at any time this leads to cause disconnections by the external party.

V.COUNTERMEASURES OF SECURITY ISSUES

Security as the fundamental goal in the security information system. These countermeasures are achieved the security policy by the service providers [2].

Confidentiality is the aspect which prevents the other user from accessing the sensitive information of the particular user.

Integrity: The attackers are not able to do the malfunctions such as modification, destruction or creation of data.

Availability: The authorized user gets the required information.

Legitimate: The services is used or accessed by only authorized user.

Accountability: The users are responsible for security related services when the user are linked when necessary.

Authenticity: The user must supply their identity for their usage of services, the unauthorized user are not able to use the resources.

Non-repudiation: It ensures that a user can prove the transmission or reception of the data by another user.

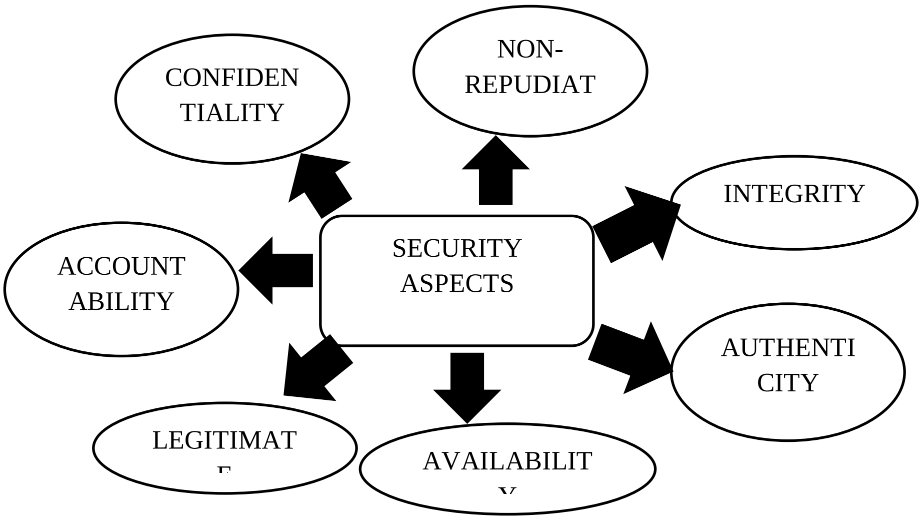

Fig 3: Security counter measures

VI.TECHNIQUES AND REQUIREMENTS OF SECURITY

The security issues to distributed systems as number of valid requirements such as identification and authentication by using authentication mechanisms like passwords, cryptographictechnique. In regard of data security in mobile computing security requirements becomes a highly important aspect than in the traditional computing. Some of the requirements are included,

Encryption : The message or the information in the mobile devices must be encrypted by using encryption key to save from the third-party or unauthorized users to access the information when the data are encrypted then the information's secure from the attacker. This encryption contributes the security aspect of confidentiality and integrity.

Standards: The user of mobile devices must have an assurance of protection of device and has the requirements like locking,antivirus,backups and password protection.

Network Access Control:This checks the mobile devices which is in the connection with the network for any malicious code or infection which damages the device.

Control Access:Control access to functions of mobile computing systems depending on the current location of the user, and there are already some security models which identifies some functions to certain user to use these functions.

Application Sandboxing: When creating mobile applications, it determined declarative permissions which will not be changed at runtime of application, these permissions can be improve to the security aspect of mobile devices by isolation and control of application from accessing to the system or interact with other applications that may be infected by malware code and virus, it also contributes to determine of resources that may be shared [3].

Memory Randomization: Memory Randomization or Address Space Layout Randomization (ASLR) which is also prevent malicious code or virus by locating the memory of application randomly, this has an important role in preventing malicious code or virus from knowing the specific memory location of the application or important memory which want to attack it [3].Some of the following steps which increase the security aspects of mobile devices which are, [3]

- Before downloading data or software, it should know the trust vendors who provide original version of software because there is some of unprotected software from external party.
- It should be aware of free applications that are popular but unofficial versions, because it may be an external party used the popularity of the original brand for nefarious purposes.
- The user should know the risk factor when they use Wi-Fi, were the attackers hack their sensitive information.
- There makes a note when the user come across with their delayed email and text message and diminished battery life in the mobile device.
- It advised to make a note of the occasions when the user feels something is unusual was happening with regard to their mobile devices like delayed email and text message, and greatly diminished battery life.

VII.CONCLUSION

This paper is a literary survey of threats and security issues, still mobile computing is in need of several other technologies to safe the information from attackers and to control the theft of the data. The emergence of mobile computing has latest evolution in the areas of computing and information systems. The popularity of its devices and of many available mobile data applications. The users of mobile device as grown high day by day in number and this usage makes convenient for users. In this paper it deals with the threats and security issues of mobile devices with solutions in some extent, but still there is a need of techniques or approaches to stop the threat and issues of mobile device.

REFERENCE

[1] D. Roselin Selvarani,"Issues, Solutions and Recommendations for Mobile Device Security", *International Journal of Innovative Research in Technology &Science (IJIRTS)***.**

[2] Sonika and Sangeeta Rani" Threats and Security Issues in Mobile Computing",*International Journal of Current Engineering and TechnologyAll Rights Reserved E ISSN 2277-5161@2014 INPRESSCO.*

[3] Srikanth Pullela,**"**Security Issues in Mobile Computing"*Department of Computer Science University of Texas at Arlington*

[4] EnaamFaihan Alotaibi," Mobile Computing Security: Issues andRequirements"**,** *Manuscript received June 9, 2015; revised November 15, 2015.*

[5] Awodele Oludele,"A Survey of Mobile Cloud Computing Applications: Perspectives and Challenges ".