# MOBILE SECURITY

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.

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

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. 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.

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.

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.

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 identified easily and hare attackers may use this identity for different purposes.

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

1. Attack based on SMS and MMS

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.


## 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.

**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 close down if not required viz.—

- Digital camera

- GPS

- Bluetooth interface

- USB interface

- Removable storage etc.