Security issues in Mobile Computing

Kartik Khurana, Harpreet Kaur, Ritu Chauhan, Shalu Chauhan, Dr. Shaveta Bhatia, Prasenjit Banerjee

1, 2, 3, 4 Students, Faculty of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India
5 Associate Professor, Faculty of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India
6 Research Mentor, Accendere KMS Pvt.Ltd.

Abstract—Now a day’s mobile communication has become a serious business tool for the users. Mobile devices are mainly used for the applications like banking, e-commerce, internet access, entertainment, etc. for communication. This has become common for the user to exchange and transfer the data. However people are still facing problems to use mobile devices because of its security issue. This paper deals with various security issues in mobile computing. It also covers all the basic points which are useful in mobile security issues such as categorisation of security issues, methods or tactics for success in security issues in mobile computing, security frameworks.

Keywords — Mobile computing, Security issues, framework for mobile environment, tactics for success.

I. INTRODUCTION

The paper discussed about the concepts of mobile computing, types of security in mobile computing, it’s availability, accountability, confidentiality, etc., why is security an issue in mobile computing, the security issues based on information security, attack security, etc. and how can we overcome the issues of mobile computing using the tactics used in mobile computing by protecting the data, creating an awareness, prioritizing the awareness, etc. Mobile Computing is a technology that allows transfer of data, voice and video. Mobile computing contains mobile communications, mobile hardware, and mobile software. The birth of “mobile computing” has signalled a new era in the field of computing and information systems. The application of mobile computing now a days become universal and pervasive in business, industrial, entertainment and other market activities. Mobile computing advantage is convenience, allowing users anytime, anywhere access to information.

II. MOBILE COMPUTING

Mobile computing is basically the interaction between the mobiles users. It contains the information of creating an information platform management. The platform management is free from spatial and temporal constraints. This allows the user to access and process the information. A user can continue the access the data at anytime and anywhere.

In mobile computing the information is being processed through wireless channels. The processed units are free to move in the space while being connected with the server. This capability helps the organisation to set their offices at any location.

III. TYPES OF SECURITY ISSUES IN MOBILE COMPUTING

- **Confidentiality:**- This ensures the transmitted information only be access by the particular user and is never disclosed to unauthorized entities.
- **Integrity:** - Guarantees that information is never use useless data during transmission. Only particular users (authorized) are able to modify it.
- **Availability:**- It ensures that the intended network services are available to the intended users when needed.
Legitimacy:- Ensuring that only authorized users have access to services.
Accountability:- Ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked if and when necessary.

IV. WHY IS SECURITY AN ISSUE?

Security is very useful for every network, but in issues of mobile computing more security issues are being characteristics by of wireless transmission and portability. The following security issues are addressed such as information security, attack security.

1. Information security:- Due to information security in any security system, first need to know our enemy. Second need is to determine possible areas- weak point, vulnerabilities. To create an information security system, the following questions are need to be answer:-
   • Who is the enemy (attacker)?
   • What are the vulnerabilities?
   • What are the negative links in the system?
   • How to give special protection?
   • To save our properties from attack?

After all these questions still there is no complete security. What may emerge to be a complete security in one reference may not be complete security in another. Therefore, while constructing a security a system, we need to reach at a proper balance between the answer emerging from the above question. In a mobile environment, the user roams through different network with different security infrastructure.

Some components of information security are:-

- Non-repudiation- Authentication and non-repudiation have some overlapping assets. Authentication is a process by which we check the identity of the parties involved in a transaction and in non-repudiation identity of these parties will identify beyond any point of doubt. It can be considered as authentication with formal record. Records have legal bindings like a signature in a cheque, using digital signatures.
- Trust- To handle trust based security management is necessary. It involves developing a security policy and verifying that the credentials fulfil the policy. Also there is need of delegation of trust to third parties, and reasoning about user's access rights.

2. Attacks:- Due to attack security, a security system is a system to defend our properties from attack. In the physical word, these attacks are carried out at the weak points in the defence system. Like in the electronic world, attacks are carried out at the point of vulnerability. When the vulnerability is exploited for some interest or selfish motive, it is an attack on the system.

Attack on dynamic assets can be of the following types:-

- Interception- An unauthorised party gaining access to an asset will be part of this attack. This is an attack on confidentiality.
- Modification- An authorised party gaining control of an asset and tempering with it is part of this attack. This is an attack on integrity.
- Interruption- An asset is destroyed or made unusable. This is an attack on availability.
- Fabrication- An unauthorised party inserts copied objects into the system.
V. TACTICS (METHODS) FOR SUCCESS

Privacy and security related to mobile computing-based solution is more vulnerable target for hackers and malicious users as mobile computing based solutions come to the fore over the public Internet. Many big players suffer from severe attacks on the Internet and safety breakdowns. Based on nothing is completely safe from the most recent mobile computing project experiences on the Internet, following the implementation of the strategy should help you to move easily.

These detection services solutions have several benefits:
To improve investigation of harmful code.
- To decrease the circulation of resources in mobile systems.
- To decrease the Software complexity of mobile system.
- Only validated data should be downloaded and the applications with unusual activity should be rejected.

The following strategies can be used to reduce to the security issues in mobile computing:
1. The Prioritize goals and set the risk durability
In this process the data assets are protecting in work places. It is a challenge for office workers for many particular sets. There is no such things which are 100% secure.

2. Safe the data with control security plan.
For organisation security plan is no easy, it involves working to understand threatening scenarios (such as hacking cyber crime strikes, media and social scandals) and protecting organizations against these threats, both policy and technology require it occurs.

3. Encourage the culture of security appreciation.
The irresponsible mistakes of a user’s will affect the Master Plan of the Chief Security Officer. This is the main reason why all users should work in the group with safety professionals ensuring safety of the business.

VI. SECURITY FRAMEWORKS FOR MOBILE ENVIRONMENT

- **3GPP:** 3rd generation partnership project is a cooperation between a set of group of telecommunication organizations, which are known as organization partners. The beginning or opening scope of 3GPP was to generate a third organisation (3G) mobile phone system definition based on the world wide system developed for mobile communication.
  To execute an attack in a wireless wide area network, the conflicting has to obtain one or more of the following capabilities.
  1. **Eavesdropping:** The attacker can be log on to the wireless network and get access to sensitive data. It happen if wireless network was not that much secure and also the information was not encrypted.
  2. **Man-in-the-middle:** It is an attack where attacker secretly transmit and possibly modify the communication between two parties. Data is sent from A (computer) to B (server/website).

- **Smartcard security:** Smartcard and enterprises system provide a large advantage of the portable and secure storage of data and value. The integration of smartcard in our system introduces issues of their own security management.
  Types of application in smartcard security FAR AND WIDE.
Smartcard encrypted data offers and the ability to store unknown (secret) information for the purpose of authenticating the card holder. There are different applications used in smartcard example: sim card in a mobile phone.

ETSI standard 03.48 identify procedure for sim card to be used as a security engine.

- **RFID security:** Radio frequency application (RFID) technology is a non-contact, automatic identification technology that uses radio signals to identify, track, sort and detect various items without the need for direct contact, including goods vehicles, goods and property or line of sight contact. RFID reader place beyond the distance of more than 10cm should not be able to read the content of e-passport however in reality it was the radio tags readable distance is as large as 30 feet. This makes the security information in the e-passport.

There are two components:

1. Modulating and demodulating radio signals.
2. Receive and transmit signals.

- **Mobile virus:** Mobile virus is malicious software that targets mobile phone or wireless-enable personal digital assistant of something (PDA’s) due to system quality is destroyed and loss or leakage of private information, since wireless phones and PDA networks have become more common and complexity has increased. It has become increasingly difficult to ensure their safety and security against electronic attacks such as viruses or other virus.

- **Mutual and Spacial Authentication:** Mutual authentication or two way authentication refers to two parties for each others authentication at same time, some protocols are optional in one default mode and the other. Most mutual authentication is machine-to-machine, export for the occasion that whether user will notice (or vare), it remote authentication fails.

Mutual authentication is two types:

2. User name-password based.

**VII. CONCLUSION**

Mobile computing is an important evolving technology as everyone is dependent on mobile these days. In this paper, security is a major category for the development in future as secure mobile computing would be a long term ongoing research topic. There are many security solutions which are available for securing information security and attack security, but no one is able to claim to resolve 100% security problems, or even most of them. Therefore this paper shows the comparative study of important security issues in mobile area.
ACKNOWLEDGMENT

We want to thanks Prasenjit Banerjee and Dr. Shaveta Bhatia for their constant support and advises during the writing of this paper.

REFERENCES


