ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Security Challenges in Mobile Computing

[I]Yasham Singhal, [II]Saloni Singh, [III]Varsha Mathpal
[I]Software Developer, Tk20 (India) Private Limited, Chandigarh, India
[II,III]B.Tech Student, CSE, College of Engineering Roorkee, India

Abstract
Currently, mobile application and computing are gaining a high momentum and playing a significant role in enhancing the internet computing infrastructure. With the rapid advances in wireless communication and portable computing devices, a new computing paradigm, which is called mobile computing, has evolved. This paper presents security challenges in mobile computing and some investigated issues have been presented here concerning the security of mobile computing system, within the framework of the categories of mobility, disconnections, data access modes and scale of operation.
In contrast to previous work which concentrates on security in wireless communications, we focus on the security of intersections which are built upon the underlying wireless communication medium.

Keywords
Mobile Devices, Mobile Communication, Mobile networks, Mobile Computing, Communication Security

I. Introduction

Mobile computing is a human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Mobile computing is the ability to use computing capability without a pre-defined location and connection to a network to publish and subscribe to information. Mobile computing as a generic term describes the ability to use the technology to wirelessly connect and use centrally located information and application software through the application of small, portable, and wireless computing and communication devices.
The birth of "mobile computing" has signalled a new era in the field of computing and information systems. The concept of mobile computing is derived from the realization that as computing machinery decreases in size thus increase in computing power users will demand these machinery to be part of their everyday life for carrying-out of their everyday tasks. Researchers in this new field envisage that mobile computing units, such as today's laptops and palmtops, in the future will be communicating with each other via wireless networks, whilst providing location transparency to the user. This notion of transparency is carried-over from the fact that in distributed computing, the user is unaware of the remote physical location of the resources which are being used by the distributed computing system.

Fig.1: Distributed Computing System

The application scope of mobile devices is increasing day by day which creates new challenges for information and security. Therefore, how to protect the security of information and applications about mobile devices becomes an exigent problem. The growth of mobile computing network is leading to new security challenges.

II. Methodology

The selection criteria through which we evaluated study sources is based on the research experience of the authors and in order to select these sources we have considered certain limitation: studies included in the selected sources must be related to our problem and these sources must be web-available.
The various protocols for mobile ad-hoc networks are available. The Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. Source-Initiated on-demand routing creates route only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. Another step in the search process is performed by searching the related work area of the selected papers to improve the review potency by confirming that no helpful reference is failed to notice during the explore process. Once the sources had been defined, it becomes necessary to describe the process and the criteria for study selection and evaluation.

III. Mobility and Security

The fact that both users and the data that they carry have become a mobile component in computing has in itself introduced a set of security problems different to that in traditional computing. In the traditional case of fixed (non-mobile) computing physical protection could easily be afforded by making a computer and database system physically isolated from the other components in the environment . In such a 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. In mobile computing this form of isolation and self-sufficiency is difficult to achieve due the relatively limited resources available to a mobile unit, thereby necessitating it to communicate with the mobile support station. The mobility of users and the data that they carry introduces security problems from the point of view of the existence and location of a user (which is deemed to be data in themselves.) and

the secrecy and authenticity of the data exchanged between users and between a user and a fixed host. More specifically, a user on a mobile wireless network may choose to have the information concerning his or her existence treated as being confidential. That is, a user may choose to remain anonymous to the majority of other users on the network, with the exception of a select number with whom the user often interacts. This problem of user anonymity in mobile computing is related to a more difficult problem of the trust level afforded by each node in the wireless network and the problem of the security of location data concerning a user when the location data is stored or transferred between nodes as the user moves in a nomadic fashion. These nodes must provide some assurance to the user about his or her anonymity, independent of the differing levels of trust that may exist for each node. This requirement is of particular importance in the case of a user that crosses between two zones which are under two nodes respectively, each having a different trust level. Equally important is the secure transfer of data between databases at nodes which hold location data and other information or parameters in the user profile. Here all traffic internal to the network and transparent to the nomadic user must be maintained secure and authentic.

IV. Security Challenges in Mobile Security

The security challenges in the mobile internet were discussed. The key objectives were to analyse the security problems to develop appropriate secure solutions related to all layers to implement sample prototype solutions and finally to stimulate the standardization process.

We can find a lot of information on the internet, such as information from companies, research institute or governmental organizations. Along with this useful information some of the information must be considered garbage but major problem is that it is hard for the user to know which information he can trust even when he knows an institution is trustworthy, since the information (or the website) might be forged.

Protocol e.g. IPSec or SSL/TLS and some layer 2 protocol like 802.11 and Bluetooth includes securities which are known and standardized. But to handle public key information in a very large scale with many communication channels is still very difficult. Rapid changes in the network topology make the job even harder. It is also unclear how security mechanisms for communication like IPSec cooperate with mobile IP and firewalls. Due to the increasing computation capabilities of PCs and workstations efficient cryptographic algorithms in low power environments as they are often found in Ad hoc networks remain unsolved and present. It is too complicated to use security mechanisms; people invent tricks like writing passwords into their address book under "s" like secret. Many people are just frustrated because of the amount of passwords and PINs they have to remember.

A. Security issues in Mobile Devices

Mobile devices should be given serious consideration because issue of security act as an obstacle in the development of mobile services. Every security issue needs to be addressed at the very outset of the service development process. The main mobile security threats for the developers of mobile services include the complexity of technical solutions, illegal copying of programs and content and threats provided by the Internet.

B. Security issues in Mobile Network

Mobile networks are being driven by the need for providing network access to mobile or wandering devices. Although the need for wireless access to a network is evident, new problems are inherent in the wireless medium .Wireless however does not imply mobility. There are wireless network in which both ends of communication are fixed such as in wireless local loops. Thus a study of wireless data networks has its own scope different from networking system in general

C. Security issues in Mobile Communication

Wireless devices such as mobile phones, PDAs and pagers are less secure than their wired counterparts. This is because of bandwidth, memory and processing capabilities. The other reason is that interruption of the data which is send into the air. Establishing of secure wireless communication channel is one of the major requirements in the PCs. Some of the important issues which need attention in designing security scheme for mobile communication are such as autonomy of communicating entities, mobility of the users and restriction of hardware.

V. Conclusion

In this study different articles and conferences were reviewed in order to provide a detailed view of security challenges in mobile devices, networks and communication. It is found that security of mobile devices is a very serious issue. This area needs proper attention of the researchers to overcome the security issues in this domain. None of the work fully solves the whole problem because of the poor interface of mobile devices, development in mobile networks and the latest technologies in mobile communication. In future these mobile devices will access different networks. Therefore, how to achieve new security challenges is a thinkable question.

VI. Acknowledgement

We wish to thank Mr. Pankaj Kumar, Assistant Professor in Computer Science Department in College of Engineering Roorkee for his help in reviewing and improving this research paper.

References

[1] Sharad Kumar Verma, Dr. D.B. Ojha-An Identity-Based Broadcast Encryption Scheme for Mobile Ad Hoc Networks. Available:- http://www.ijceronline.com/papers/Vol2_issue5/CK02516951698.pdf

[2] Swarnpreet Singh, Ritu Bagga,Devinder Singh, Tarun Jangwal -Architecture Of Mobile Application, Security issues And Services Involved In Mobile cloud Computing Environment, Available- http://www.ijcer.org/index.php/ojs/article/viewFile/9/7

[3] Jun-Zhao Sun, Douglas Howie, Antti Koivisto, and Jaakko Sauvola-A Hierarchical Framework Model of Mobile Security, Available-http://www.mediateam.oulu.fi/publications/pdf/76.pdf

[4] http://www.academia.edu/Documents/in/Security_in_Mobile_Payments_Security_in_Proximity_Mobile_Payments

[5] Jon Oltsik-Addressing Mobile Device Securityand Management Requirementsin the Enterprise, Available-http://investor.juniper.net/files/doc_downloads/resources/JNPResg-addressing-mobile-sevice[1].pdf