International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

General Article

# Threats and Security Issues in Mobile Computing

Sonika[Å*] and Sangeeta Rani[Å]

BLS Institute of Technology Management, Bahadurgarh- 124507,NCR (Haryana), India

Accepted 05 Oct 2014, Available online 10 Oct 2014, **Vol.4, No.5 (Oct 2014)**

***Abstract***

*During the last decade the decrease in the size of computing machinery, coupled with the increase in their computing power has led to the development of the concept of mobile computing. Mobile Computing is a generic term is evolved in modern usage such that it requires that the mobile computing activity be connected wirelessly to and through the internet or to and through a private network. Now a days Mobile internet has changed the way we work and we live, one can easily reached people around the globe instantly, from any device, over any network. The adoption of Internet services has shown to be more difficult due to the difference between the Internet and the mobile telecommunication system. Security is the key issue that needs to be considered, which comes into picture once. The communication channel is set up. This paper provides an insight on threats, challenges and recent trends security issues in mobile computing.*

***Keywords:*** *Mobile computing, mobile computing security, wireless mobile communication, WI-Fi network, KSSL Protocol*

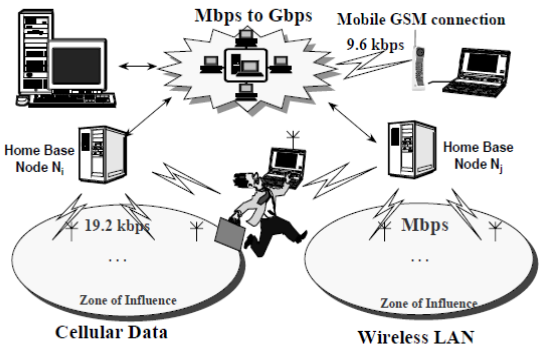
## 1. Introduction

Mobile computing is a form of human–computer interaction by which a computer is expected to be transported during normal usage. Mobile Computing is a variety of wireless devices that has the mobility to allow people to connect to the internet, providing wireless transmission to access data and information from where ever location they may be. Mobile computing has three aspects: mobile communication, mobile hardware, and mobile software. The first aspect addresses communication issues in ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. The second aspect is on the hardware, e.g., 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. With 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.

## 2. 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.




Mobile Computing Environment

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

*Correspoding author: **Sonika**

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.

Another potential security problem lies in the possibility of information leakage through the inference made by an attacker masquerading as a mobile support station with or without the aid of a subverted mobile support station. The attacker which masquerades as a mobile support station may issue a number of queries to the database at the user's home node or to database at other nodes, with the aim of deducing parts of the user profile containing the patterns and history of the user's movements. Here again, security techniques are required both for the databases and for the identification of users and mobile support stations. Any scheme to be used must ensure that any queries submitted to a given database at a user's home-base is accompanied by sufficient proof that the user approves of the queries submitted by the (foreign) mobile support station controlling the zone under which the user is currently roaming or passing through. It is, therefore, not unreasonable to assume that some method of delegation of rights will be employed between the user and the mobile support stations (and fixed hosts) in the network.

Related to the management of these databases and the provision of performance transparency for the nomadic user is the issue of replication of certain parameters and user profiles with the aim of replicating the environments surrounding the user. Thus, as theuser roams across zones, the user must not experience a degradation in the access and latency times. Again, security must be considered in the context of replication, both from the trust level of the mobile support stations and fixed hosts and from the point of view of data leakage. In general, as sensitive data is replicated across several sites, the security risks are also increased due to the multiplication of the points of attack.

## 3. Threats to Mobile Computing

Mobile computing brings with it threats to the user and to the corporate environment. From personal information to corporate data, mobile devices are used for a wide variety of tasks by individuals and companies. Mobile devices have added a new threat to the corporate landscape as they have introduced the concept of bring your own device . While this is not necessarily an entirely new concept, the wide acceptance of bring your own device with mobile devices has created a paradigm shift, where the security and safety of the device is not necessarily to protect the corporate data, but to keep the personal data out of the hands of corporate management.

*1. Data Loss from lost, stolen, or decommissioned devices:* By their nature, mobile devices are with us everywhere we go. The information accessed through the device means that theft or loss of a mobile device has immediate consequences. Additionally, weak password access, no passwords, and little or no encryption can lead to data leakage on the devices. Users may also sell or discard devices without understanding the risk to their data. The threat level from data loss is high, as it occurs frequently and is a top concern across executives and IT admins.

*2. Information stealing mobile malware:* Android devices, in particular, offer many options for application downloads and installations. Unlike iOS devices, which need to be jailbroken, Android users can easily opt to download and install apps from third-party marketplaces other than Google's official Play Store marketplace. To date, the majority of malicious code distributed for Android has been disseminated through third-party app stores. Most of the malware distributed through third-party stores has been designed to steal data from the host device. This threat level is high, as Android malware in particular is becoming a more popular attack surface for criminals who traditionally have used PCs as their platforms.

*3. Data Loss and data leakage through poorly written third-party applications:* Applications for smartphones and tablets have grown exponentially on iOS and Android. Although the main marketplaces have security checks, certain data collection processes are of questionable necessity; all too often, applications either ask for too much access to data or simply gather more data than they need or otherwise advertise. This is a mid-level threat. Although data loss and leaking through poorly written applications happens across mobile operating systems.

*4. Vulnerabilities within devices, OS, design, and third-party applications:* Mobile hardware, OS, applications and third-party apps contain defects (vulnerabilities) and are susceptible to exfiltration and/or injection of data and/or malicious code (exploits). The unique ecosystem inherent in mobile devices provides a specialized array of security concerns to hardware, OS, and application developers, as mobile devices increasingly contain all of the functionalities attributed to desktop computing, with the addition of cellular communication abilities. This is a mid-level threat; although the possibility is high, the number of exploits is not.

*5. Unsecured WiFi, network access, and rogue access points:* This has increased the attack surface for users who connect to these networks. In the last year, there has been a proliferation of attacks on hotel networks, a skyrocketing number of open rogue access points installed, and the reporting of eavesdropping cases. This threat level is high. Increased access to public WiFi, along with increased use of mobile devices, creates a heightened opportunity for abuse of this connection.

*6. Unsecured or rogue marketplaces:* Android users can easily opt to download and install apps from third-party

marketplaces other than Google's official Play Store marketplace. To date, the majority of malicious code distributed for Android has been distributed through third-party app stores. This threat level is high: Android malware in particular is being distributed through these marketplaces more and more frequently.

*7. Insufficient management tools, capabilities, and access to APIs (includes personas):* Granting users and developers access to a device's low-level functions is a double-edged sword, as attackers, in theory, could also gain access to those functions. However, a lack of access to system-level functions to trusted developers could lead to insufficient security. Additionally, with most smartphone and tablet operating systems today, there is little, if any, guest access or user status. Thus, all usage is in the context of the admin, thereby providing excessive access in many instances. This is a mid-level threat.

*8. NFC and proximity-based hacking:* Near-field communication (NFC) allows mobile devices to communicate with other devices through short-range wireless technology. NFC technology has been used in payment transactions, social media, coupon delivery, and contact information sharing. Due to the information value being transmitted, this is likely to be a target of attackers in the future. The threat level is low, as the threat is still in the proof-of-concept phase.

## 4. Security Countermeasures

Secure mobile computing is critical in the development of any application of wireless networks.

*Security Requirements*

Similar to traditional networks, the goals of securing mobile computing can be defined by the following attributes: availability, confidentiality, integrity, authenticity and non-repudiation.

*Availability* ensures that the intended network services are available to the intended parties when needed.

*Confidentiality* ensures that the transmitted information can only be accessed by the intended receivers and is never disclosed to unauthorized entities.

*Authenticity* allows a user to ensure the identity of the entity it is communicating with. Without authentication, an adversary can masquerade a legitimate user, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of users.

*Integrity* guarantees that information is never corrupted during transmission. Only the authorized parties are able to modify it.

*Non-repudiation* ensures that an entity can prove the transmission or reception of information by another entity, i.e.,a sender/receiver cannot falsely deny having received or sent certain data.

In ad hoc networks, mobile hosts are not bound to any centralized control like base stations or access points. They are roaming independently and are able to move freely with an arbitrary speed and direction. Thus, the topology of the network may change randomly and frequently. In such a network, the information transfer is implemented in a multi-hop fashion, i.e., each node acts not only as a host, but also as a router, forwarding packets for those nodes that are not in direct transmission range with each other. By nature, an ad hoc network is a highly dynamic self-organizing network with scarce channels. Besides these security risks, ad hoc networks are prone to more security threats due to their difference from conventional infrastructure-based wireless networks.

*The Lack of Pre-fixed Infrastructure* means there is no centralized control for the network services. The network functions by cooperative participation of all nodes in a distributed fashion. The decentralized decision making is prone to the attacks that are designed to break the cooperative algorithms. A malicious user could simply block or modify the traffic traversing it by refusing to cooperate and break the cooperative algorithms. Moreover, since there are no trusted entities that can calculate and distribute the secure keys, the traditional key management scheme cannot be applied directly.

*Dynamically Changing Topology* aids the attackers to update routing information maliciously by pretending this to be legitimate topological change. In most routing protocols for ad hoc networks, nodes exchange information about the topology of the network so that the routes could be established between communicating nodes. Any intruder can maliciously give incorrect updating information. For instance, DoS attack can be easily launched if a malicious node
floods the network with spurious routing messages. The other nodes may unknowingly propagate the messages.

*Energy Consumption Attack* is more serious as each mobile node also forwards packets for other nodes. An attacker can easily send some old messages to a node, aiming to overload the network and deplete the node's resources. More seriously, an attack can create a *rushing attack* by sending many routing request packets with high frequency, in an attempt to keep other nodes busy with the route discovery process, so the network service cannot be achieved by other legitimate nodes.

*Node Selfishness* is a specific security issue to ad hoc network. Since routing and network management are carried by all available nodes in ad hoc networks, some nodes may selfishly deny the routing request from other nodes to save their own resources (e.g., battery power, memory, CPU).

## 5. Security Issues Involved In Mobile Computing

i) Mobile security or mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal information now stored on the smart phone. More and more users and businesses use smart phones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smart phones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

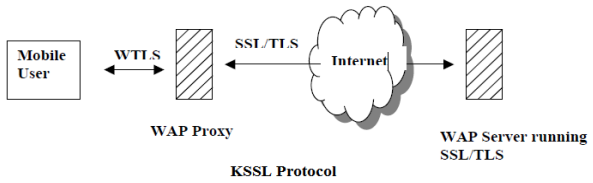
**Table 1** Security Vulnerabilities of a general mobile computing system

| | *Mobile units* | *Over the air* | *Wired hosts* |
|---|---|---|---|
| *Physical vulnerabilities* | small size and weight, portability, exposure in hostile places | random happenings that easy affect wireless communications | different locations |
| *Natural vulnerabilities* | exposure in outdoor environmental conditions | affected from weather situations, hand-offs between cells | unknown boundaries, many points to attack |
| *H/W and S/W vulnerabilities* | not enough hardware controls and resources | | heterogeneity, shared use of resources |
| *Communications vulnerabilities* | dependence on the communication infrastructure | broadcasting | |
| *Human vulnerabilities* | away from technical support and management, lack of attention | unlimited capability for physical access | |

ii) All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smart phones that can come from means of communication likes SMS,MMS,WIFI NETWORKS. There are also attacks that exploit software vulnerabilities from both the web browser and operating system.

iii) Different security counter-measures are being developed and applied to smart phones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

iv) One of the key issues of these being, confidentiality and authentication, where the user must be protected from unauthorized eavesdropping. The goal of authentication protocol is to check the identity of other users or network centers before providing access to the confidential information on the users side. When designing any security protocol, there are certain conditions that need to be considered. Firstly, the low computational power of the mobile users and secondly, the low bandwidth available. Therefore, it is important to design the security protocols so as to minimize, the number of message exchanges and the message size. a few authentication protocols that were proposed to provide security between the users and the network. These protocols are based on the use of certificates, which are built on the concept of security keys (cryptography). Another protocol that is discussed in this paper is the KiloByte Secure Socket Layer (KSSL) protocol, which is an extension of Secure Socket Layer (SSL) protocol used for wired networks.




## 6. Security Controls in Mobile Computing Systems

Our work on the security of mobile computing aims to address the problems pertaining to the security of information within the following three sub-areas of the mobile environment:

1. The security of information residing in the mobile units, considering device constraints,
2. The security of information as it travels 'over the air' between mobile units and mobile support stations. An important consideration in this area is the power consumption of the algorithms that implement this secure data transfer.
3. The security of information within the rest network (wired hosts). This includes the security of databases holding control data used for the operations and management of the mobile wireless network.

In the tables 1, we summaries for each of the above sub-areas the major security vulnerabilities that a general mobile computing system is prone to.

## Conclusions

This paper presents an analysis of threats and security issues which demands thorough data-centric threat-risk and security Assessments , incident handling planning and preparation and user and administrator training. Mobile computing still requires many other technologies to be collaborated for fulfilling the changing needs of users worldwide to protect the information from unauthorized users and control the fraud. With these efforts relatively new and not yet developed to its full extent, service providers are hoping to keep security development in pace with other developmental aspects of wireless technology.

Future work includes a systematic definition of different security policies that are used by different backbone networks. Further work also includes the implementation of special authentication and access control techniques.

## References

Mobile Communications, *Jochen Schi*ller (2000), Addison-Wesley.

D. P. Agrawal and Q-A. Zeng (2002.), *Introduction to Wireless and Mobile Systems*, Brooks/Cole publisher

Y. C. Hu and D. B. Johnson and A. Perrig, *SEAD: Secure Efficient Distance Vector Routing in Mobile.*

Wireless Ad-Hoc Networks (2002), *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02)*, pp. 3-13.

Campbell, R.; Sturman, D. and Tock, T. (1994) *Mobile Computing, Security and Delegation.* [6]*International Workshop on Multi-Dimensional Mobile Communication*s, Japan. html.

Duchamp, D. (1992) Issues in Wireless Mobile Computing. *Proceedings Third Workshop on Workstation Operating Systems*, April 1992, 2-10.

Forman, G.H. and Zahorian, J. (Apr 1994) *The Challenges of Mobile Computing. IEEE Computer*, April 1994, 38-47.

Asokan (Apr. 1995), Security Issues in Mobile Computing, Univ. of Waterloo, Dept. of Computer Science, *Technical Report CS690B.*

Charlie Perkins, *Mobile IP and Security Issue: An Overview*

Mavridis Pangalos, *Security Issues in a Mobile Computing Paradigm.*

G.H. Forman, J. Zahorjan, *The Challenges of Mobile Computing, IEEE Computer*, V 27, N 4, pp. 38-47

Talukder and Yavagal,*Mobile Computing: Technology, Applications and Service Creation*

Reza B'Far, *Mobile Computing Principles*

PerkinsT.*Mobile-IP Design principles and Practices*

Imielinski and H. Korth.*Mobile Computing*