Mobile Computing – An Introduction with Issues in Mobile Security

Dr. Priyank Gokani
Associate Professor
Department of Information Technology
Dr. V. R. Godhaniya College of IT
Porbandar

A B S T R A C T

As more and more people enjoy the various brought by mobile computing, it is becoming a global trend in today's world.at the same time, securing mobile computing has been paid increasing attention. During the last decade in the size of computing machinery, coupled with the increase in their computing power has lend to the development of the concept of mobile computing. It allows mobile users versatile communication with other people and expedient notification of important events, much more flexibility them with cellular phones. The many issues to be dealt with stem from three essential properties of mobile computing: communication, mobility and portability. In this paper, we discuss the security issues in mobile computing.

1. INTRODUCTION

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage.The birth of "mobile computing" has signaled a new era in the field of computing and information systems. A technology that allows transmission of data, via a computer, without having to be connected to a fixed physical link.

As wireless communication takesplace mainly through the radio signals rather than wires, it is easier to intercept or eavesdrop on the communication channels. Therefore, it is important to provide security from all these threats. There are different kinds of issues within security like confidentiality, integrity, availability, legitimacy, and accountability that needs to be individually taken care off.The last few years have seen a true revolution in the telecommunications world. Besides the three generations of wireless cellular systems, ubiquitous computing has been possible due to the advances in wireless communication technology and availability of many light-weight, compact, portable computing devices, like laptops, PDAs, cellular phones, and electronic organizers.

1.1. Mobile Connectivity

The mobile connectivity between two nodes exists if they are continuously connected through wireless channel, and can utilize the channel without being subjected to spatial and temporal constraints.

2. DIFFERENT TYPES OF MOBILE SYSTEMS

In many ways, mobile computing has several characteristics reminiscent of distributed systems. In order to understand mobile systems, one must first understand where the similarities and the differences of distributed and mobile systems lie. The following section is an explanation of the different types of distributed systems ranging from the traditional type to nomadic, ad-hoc and finally ubiquitous ones.

2.1. TraditionalDistributed Systems

Traditional distributed systems consist of a collection of fixed hosts that are themselves attached to a network– if hosts are disconnected from the network this is considered to be abnormal whereas in a mobile system this is quite the norm. These hosts are *fixed* and are usually very powerful machines with fast processors and large amount of memory. The bandwidth in traditional systems is very high too. Traditional distributed systems also need to guarantee non-functional requirements such as scalability (accommodate a higher load at some time in the future), openness (possibility to extend and modify the system easily), heterogeneity (integration of components written using different programming languages, running on different operating systems, executing on different hardware platforms), fault-tolerance (recover from faults without halting the whole system) and finally resource-sharing (some form of access control).

2.2. NomadicDistributed System

This kind of system is composed of a set of mobile devices and a core infrastructure with fixed and wired nodes. Mobile devices move from location to location, while maintaining a connection to the fixed network. There are problems that arise from such shifts in location. The mobile host has a home IP address and thus any packets sent to the mobile host will be delivered to the home network and not the foreign network where the mobile host is currently located. Such problem can be solved by forwarding packets to the foreign network with the help of Mobile IP. Nevertheless, Mobile IP also suffers from efficiency (routing issues), QoS, security (authentication of mobile host at foreign network and end-to-end security required) and wireless access (reduced capacity) problems. These systems are susceptible to the uncertainty of location, a repeated lack of connections and the migration into different physical and logical environments while operating. However, compared to ad-hoc networks, nomadic systems still have comparatively reliable connections and services since most of these are actually supported by the fixed infrastructure ("backbone") of the network.

3. SECURITY ISSUES

Many authors have presented classifications of security issues in communication networks. There are five fundamental goals of security in information system.

Confidentiality:
Preventing unauthorized users from gaining access to critical information of any particular user.

Integrity:
Ensures unauthorized modification, destruction or creation of information cannot take place.

Availability:
Ensuring authorized users getting the access they require.

Legitimate:
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. The way these goals are achieved depends on the security policy adopted by the service providers.

3.1. Security Risks of Infrastructure-Based WLANs

Because a wireless LAN signal is not limited to the physical boundary of a building, potential exists for unauthorized access to the network from personnel outside the intended coverage area. Most security concerns arise from this aspect of a WLANs and fall into the following basic categories:

Limited Physical Security

Unlike traditional LANs, which require a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point (AP) device. As shown in Figure 1 an access point communicates with devices equipped with wireless network adaptors and connects to a fixed network infrastructure. Since there is no physical link between the nodes of the wireless network and the access point, the users transmit information through the "air" and hence anyone within the radio range (approximately 300 feet for 802.11b) can easily intercept or eavesdrop on the communication channels. Further, an attacker can deploy unauthorized devices or create new wireless networks by plugging in unauthorized clients or setting up renegade access points.

Constrained Network Bandwidth

The use of wireless communication typically implies a lower bandwidth than that of traditional wired networks. This may limit the number and size of the message transmitted during protocol execution. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, corrupting the signal until the network ceases to function. Since the aim of this type of attack is to disable accessing network service from the legitimate network users, they are often named denial of service (DoS) attack. Denial of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

4. SECURITY COUNTERMEASURES

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

4.1 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.

5. TACTICS FOR SUCCESS

After the selection decision for a particular mobile computing application has been made, implementing the system just as carefully will help to ensure that the end users are satisfied and full value is realized. The following implementation tactics, based on the most recent mobile computing project experiences, should help projects move smoothly

5.1. Understand The Integration Of Workflow, Information Flow, And Technology

Mobile computing is not the entire solution; it addresses specific tasks within the care delivery process. Understanding the points where technology is provided and the information collected or displayed for the end user will lead to a clear map of the necessary changes in the current process and roles. In many projects, implementing the process, roles, and responsibility changes is far more challenging than installing the new technology.

5.2. Set User Expectations

Take the time to under-stand, document, and set expectations related to each functionality and technology that will be installed. Many device manufacturers and application vendors claim incredible functionality and access to information. Remember that mobile does not necessarily mean wireless, real-time access to data. Make sure that end users are not led to believe that the application is going to give them access to the same services and functionality that they have on their PCs with wired connections. Mobile computing will give them basic functions with the added benefit of mobility.

5.3. Pilot The Application

A great implementation advantage with mobile computing is that piloting is possible. The cost for the handheld devices, software, and basic data synchronization interfacing is very low, especially if the vendor is willing to partner with the organization to gain experience with implementations and have reference sites. By starting small, users get a clear under-standing of how mobile computing impacts their workenvironment. Pilot implementations identify process and technology adjustments that will improve user acceptance and the overall success of the project when it is rolled out.

5.4. Personal Digital Assistant (PDA)

A personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager. PDAs are largely considered obsolete with the widespread adoption of smart phones. Nearly all current PDAs have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, all current models also have audio capabilities enabling use as a portable

media player, and also enabling most of them to be used as mobile phones. Most PDAs can access the Internet, intranets or extranets via Wi-Fi or Wireless Wide Area Networks. Most PDAs employ touch screen technology.

Smart Phone:

Smart-phone is the trend of unified communications which integrate telecom and Internet services onto a single device because it has combined the portability of cell-phones with the computing and networking power of PCs. As illustrated in Figure 1, smart-phones, as endpoints of both networks, have connected the Internet and telecom networks together.

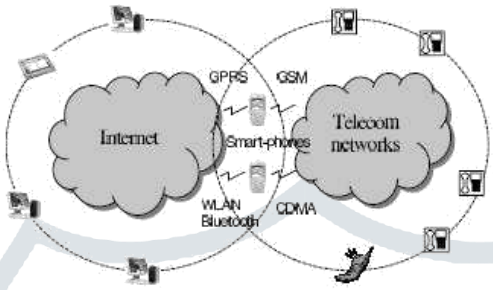

Fig 1 : Mobile Network

5. CONCLUSION

Mobile computing is an important, evolving technology. It enables mobile personnel to effectively communicate and interact with the fixed organizational information system while remaining unconstrained by physical location. Mobile computing may be implemented using many combinations of hardware, software, and communications technologies. Mobile computing technology provides anytime and anywhere service to mobile users by combining wireless networking and mobility.

In this paper we have proposed security to b e a major category for future developments in mobile computing. We have seen that many security solutions. In essence, secure mobile computing would be a long-term ongoing research topic.

REFERENCES:

1. en.wikipedia.org/wiki/**Mobilecomputing**

2.http://www.fujitsu.com/downloads/MAG/vol34-1/paper02.pdf

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

4. J. Walker, "Overview of IEEE 802.11b Security",http://www.intel.com/technology/itj/q22000/pdf/art_5.pdf.

5. Y. C. Hu and D. B. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks," Proceedings of the 4th IEEE Workshop on Mobile Computing SystemsandApplications *(WMCSA '02),* pp. 3-13, 2002.

6.Wireless and Mobile Computing, by Fran Turisco and Joanna Case, First Consulting Group Mobile Computing, by Vijay Kumar, University of Missouri-Kansas City Kansas City, MO 64110, USA.

7. Kumar, P., Satyanarayanan, M.
Flexible and Safe Resolution of File Conflicts.In Procedings of the 1995 *USENIX* Technical Conference. New Orleans, LA, January, 1995.

8. Kung, H.T., Robinson, J. On Optimistic Methods for Concurrency Control. *ACM* Transaction on Database Systems6(2), June, 1981.