ISBN-978-93-5288-834-3

Security Issues In Mobile Computing

Ankit Kumar Mishra[1], Pradeep Kumar Sah[2]
[1]*College of Computing Sciences and Information Technology (CCSIT), TMU, Moradabad*
[2]*College of Computing Sciences and Information Technology (CCSIT), TMU, Moradabad*
[1]ankitmishra988@gmail.com
[2]pradeep.mca11@gmail.com

***ABSTRACT*— In this paper, we discuss operational and security issues arising from the use of mobile components. In the present mobile communication environment, lot of research is going on, to improve the performance of issues like handoffs, routing etc. Security is another key issue that needs to be considered, which comes into picture once the communication channel is setup. Many security protocols are being proposed for different applications like Wireless Application Protocol, 802.11 etc. most of them are based on the public and private key Cryptography.**

Laptop computers, cell phones, mobile data storage devices, and similar mobile computing and communication devices have become very popular because of their convenience and portability. This has led to the creation of a new computing platform called mobile computing. However, the use of such devices in this new platform is accompanied by new security risks that must be recognized and addressed to protect the physical devices, the communication medium, and the information used. In this report security issues introduced by mobile computing has been discussed, and a summary of current existing security measures is given.

***KEYWORDS*— Mobile computing, mobile computing security**

1. INTRODUCTION

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 the provision of providing data anywhere, anytime, the need of mobile communication security increases to a great degree. As wireless communication takes place 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.

Mobile computing is a frequently used term that can be defined as having access to computing resources from anywhere using mobile devices However, the use of such devices in such a platform comes with new security risks and challenges that must be recognized and addressed to keep this new computing environment safe and secure. Mobile computing devices are capable of storing, processing, displaying, and communicating information. This information could be sensitive information, such as the identification and credit data of customers, and the mobile devices can move in and out of the boundaries of a networking environment. Mobile users have the ability to work from anywhere without being bound to any networking system. This flexibility extends the network.

2. SECURITY ISSUES

Security is a prerequisite for every network, but mobile computing presents more security issues than traditional networks due to the additional constraints imposed by the characteristics of wireless transmission and the demand for mobility and portability. We address the security problems for both infrastructure-based WLANs and infrastructure-less ad hoc networks.

2.1 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:

2.1.1 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. 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

ISBN-978-93-5288-834-3

channels. Further, an attacker can deploy unauthorized devices or create new wireless networks by plugging in unauthorized clients or setting up renegade access points.

2.1.2 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.

2.1.3 ENERGY CONSTRAINED MOBILE HOSTS

To support mobility and portability, mobile devices generally obtain their energy through batteries or other exhaustive means, hence they are considered as energy constrained mobile hosts. Moreover, they are also resource-constraint relative to static elements in terms of storage memory, computational capability, weight and size. In WLANs, two wireless clients can talk directly to each other, bypassing the access point. A wireless device can create a new type of denial of service attack by flooding other wireless clients with bogus packets to consume its limited energy and resources.

2.2 SECURITY RISKS OF INFRASTRUCTURE-LESS AD HOC NETWORKS

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.

2.2.1THE LACK OF PRE-FIXED INFRASTRUCTURE

It 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.

2.2.2 DYNAMICALLY CHANGING TOPOLOGY

It 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.

2.2.3 ENERGY CONSUMPTION ATTACK

It 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

ISBN-978-93-5288-834-3

process, so the network service cannot be achieved by other legitimate nodes.

2.2.4 NODE SELFISHNESS

It 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).

3. SECURITY COUNTERMEASURES

3.1 WLAN BASIC SECURITY MECHANISMS

The IEEE 802.11b standard identifies several security services such as encryption and authentication to provide a secure operating environment and to make the wireless traffic as secure as wired traffic. In the IEEE 802.11b standard, these services are provided largely by the WEP (Wired Equivalent Privacy) protocol to protect link-level data during wireless transmission between clients and APs. That is, WEP does not provide any end-to-end security but only for the wireless portion of the connection. Apart from WEP, other well-known methods that are built into 802.11b networks are: Service Set Identifier (SSID), Media Access Control (MAC) address filtering, and open system or shared-key authentication [3].

SSID: Network access control can be implemented using an SSID associated with an AP or group of APs. Each AP is programmed with an SSID corresponding to a specific wireless LAN. To access this network, client computers must be configured with the correct SSID. Typically, a client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations. Because a client computer must present the correct SSID to access the AP, the SSID acts as a simple password and, thus, provides a measure of security. However, this minimal security is compromised if the AP is configured to "broadcast" its SSID. When this broadcast feature is enabled, any client computer that is not configured with a specific SSID is allowed to receive the SSID and access the AP.

MAC ADDRESS FILTERING**:** While an AP can be identified by an SSID, a client computer can be identified by a unique MAC address of its 802.11b network card. To increase the security of an 802.11b network, each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client's MAC address is not included in this list, the client is not allowed to associate with the AP. MAC address filtering (along with SSIDs) provides improved security, but is best suited to small networks where the MAC address list can be efficiently managed. Each AP must be manually programmed with a list of MAC addresses, and the list must be kept up-to-date.

AUTHENTICATION: In a WLAN, an AP must authenticate a client before the client can associate with the AP or communicate with the network. The IEEE 802.11b standard has defined two types of authentication methods: open system and shared Key. Open system authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the "ANY" SSID option to associate with any available AP within range, regardless of its SSID. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. When wireless devices are configured to operate in this mode, Wired Equivalent Privacy (WEP) data encryption is used and it requires that the station and the AP have the same WEP Key to authenticate, thus preventing the client from sending and receiving data from the AP, unless the client has the correct WEP key .The two authentication modes. By default, IEEE 802.11b wireless devices operate in an open system authentication mode. Both of these authentication modes are one-way authentication, i.e., the mobile clients can be authenticated by the APs, but the authenticity of APs is not authenticated. Thereby, a rogue node may

ISBN-978-93-5288-834-3

masquerade as an AP and establish communication with the mobile nodes.

WEP-BASED SECURITY: WEP security protocol encrypts the communication between the client and an AP. It employs the symmetric key encryption algorithm, RC4 Pseudo Random Number Generator. Under WEP, all clients and APs on a wireless network typically use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. The 802.11b standard does not specify a key-management protocol, so all WEP keys on a network usually must be managed manually and are static for a long period of time. This is a well-known security vulnerability. Support for WEP is standard on most current 802.11 cards and APs. WEP specifies the use of a 40-bit encryption key. The encryption key is concatenated with a 24-bit "initialization vector" (IV), resulting in a 64-bit key. This key is input into a pseudorandom number generator. The resulting sequence is used to encrypt the data to be transmitted. However, WEP encryption has been shown to be vulnerable to several cryptographic attacks that reveal the shared key used to encrypt and authenticate data, such as IV key reuse, key stream reuse, message injection, and so on . Because of this, static WEP is only suitable for small, tightly managed networks with low-to-medium security requirements. It is clear that these traditional WLAN security that relies on SSIDs, open system or shared key authentication, MAC address filtering, and static WEP keys is better than no security at all, but it is insufficient, and a new security solution is needed to secure mobile computing.

3.2 ADVANCED WLAN SECURITY MECHANISMS

WEP2: As an interim improved solution to the many flaws of WEP, the TGI Working Group of the IEEE proposed WEP2. Unfortunately, similar to major problems with WEP, WEP2 is not an ideal solution. The main improvement of WEP2 is to increase the IV key space to 128 bits, but it fails to prevent IV replay and still permits IV key reuse. The weakness of plaintext exploits and same IV replay are the same with that in WEP. In WEP2, the authentication is still a one-way authentication mode, and the problem of rogue AP is not solved.

VIRTUAL PRIVATE NETWORKING (VPN): To further address the concerns with WEP security, many organizations adopt the virtual private network (VPN) technology. The VPN approach has a number of advantages. Firstly, it is scalable to a large number of 802.11 clients and has low administration requirements for the IEEE 802.11 APs and clients. Secondly, the VPN servers can be centrally administered and the traffic to the internal network is isolated until VPN authentication is performed. Thirdly, if this approach is deployed then a WEP key and MAC address list management is not needed because of security measures created by the VPN channel itself. This is a good solution for networks, particularly with existing VPN infrastructure for remote access.

However, though the VPN approach enhances the air-interface security significantly, this approach does not completely address security on the enterprise network. For example, authentication and authorization to enterprise applications are not always addressed with this security solution. Some VPN devices can use user-specific policies to require authentication before accessing enterprise applications. Another drawback in the VPN solution is the lack of support for multicasting, which is a technique used to deliver data efficiently in real time from one source to many users over a network. Multicasting is useful for streaming audio and video applications such as press conferences and training classes. Also, a minor issue of VPNs is that roaming between wireless networks is not completely transparent. Users receive a logon dialog when roaming between VPN servers on a network or when the client system resumes from standby mode. Some VPN solutions address this issue by providing the ability to "auto re-connect" to the VPN.

IEEE 802.11I ROBUST SECURITY NETWORK (RSN) STANDARD: To help overcome this security gap in wireless networks, the IEEE 802.11 working group instituted Task Group i (802.11i) has proposed significant modifications to the existing IEEE 802.11 standard as a long-term solution for security, called Robust Security Network (RSN). An interim draft of IEEE 802.11i is now available, known as Wi-Fi Protected Access (WPA). The draft of IEEE 802.11i standard consists of three major parts: Temporal Key Integrity Protocol (TKIP), counter mode cipher block chaining with message authentication codes (counter mode CBC-MAC) and IEEE 802.11x access control.

TKIP primarily addresses the shortcomings of WEP and fixes the well-known problems with WEP, including small initialization vector (IV) and short encryption keys. TKIP uses RC4, the same encryption algorithm as WEP to make it updateable from WEP, but it extends the IV from 24-bit to 48-bit in order to defend against the existing cryptographic attacks against WEP. Moreover, TKIP implements 128-bit encryption key to address the short-key problem of WEP. TKIP changes the way keys are derived and periodically rotates the broadcast keys to avoid the attack that is based on capturing large amount of data encrypted by the same key. It also adds a message-integrity check function to prevent packet forgeries. TKIP is part of the existing WPA industry standard [4].

4. LIMITATIONS TO MOBILE COMPUTING

- Resource constraints: Battery.
- Interference: the quality of service (QoS).
- Bandwidth: connection latency.
- Dynamic changes in communication environment: variations in signal power within a region, thus link delays and connection losses.
- Network Issues: discovery of the connection-service to destination and connection stability
- Interoperability issues: the varying protocol standards.
- Security constraints: Protocols conserving privacy of communication [5].

5. CONCLUSION

Initially, when the wireless mobile environment came into existence security was not given a priority. But, as the time passed by, the extent to which this technology is used increased. This created a need to protect the information from unauthorized users and control the fraud. In the beginning, many security protocols where proposed, which were based on cryptographic techniques. With new loopholes coming up each time, a new protocol was proposed based on the existing one, to answer the problem. Presently, many researchers are concentrating on using the wired based security protocols over the wireless mobile communication.

According to me, the present research that is going on, is trying to extend the security protocols used in wired networks to wireless mobile environment is a good step in providing high -end security. As the security protocols used in wired network have undergone heavy scrutiny over the years from various ends using these protocols in the mobile environment, would help in achieving good performance results.

Also, many wireless communication service vendors are developing new protocols and standards to provide a secured medium for the mobile users. 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.

REFERENCES

[1] "Security Issues in Mobile Computing", Srikant Pullela, Department of Computer Science University of Texas at Arlington.
[2] http://en.wikipedia.org/wiki/Mobile_computing.
[3] "Secure Mobile Computing", Dharma P. Agrawal , Hongmei Deng , Rajani Poosarla and Sugata Sanyal, Center for Distributed and Mobile Computing University of Cincinnati, Cincinnati, OH 45221-0030
[4] J. Walker, "Overview of IEEE 802.11b Security", http://www.intel.com/technology/itj/q22000/pdf/art_5.pdf.
[5] http://www.dauniv.ac.in/downloads/Mobilecomputing/MobileCompChap01L07_MobComputing.pdf.