Security Issues in Mobile Computing

Part 1

Why Security

- mobile computing systems are based on wireless networks and wireless communication technologies, the security of such systems is a major concern.

- Why need security?

Security becomes mandatory in mobile systems due to the existence of hackers, viruses, intruders and Internet-based attackers, who have easy access to such systems through the broadcast nature of wireless channels.

Security Issues in Wireless Network

- Larger security challenges are present in wireless networks than in conventional wired networks.

- Much of the security problem in wireless networks can be traced to the base stations or access points (AP), which operate without any security at all and can be easily taken out and put into wired (Ethernet) nets, exposing the data on it to everyone within its radio range.

Security Issues in Wireless Network

- The dissimilarities between wired and wireless networks make it difficult to implement the existing firewalls and other intrusion detection systems (IDS) of wired networks in wireless networks.
  - The most significant difference is that data in a wireless network are transmitted over the broadcast medium, rendering it available to all nodes in the vicinity.
  - Another major difference lies in the communication link, which is slower and of lower bandwidth. Limited battery constraints and higher costs are also major drawbacks in mobile, portable systems, giving rise to frequent disconnections.

Network Security in Wireless Systems

Network security in wireless systems can still be divided roughly into the following four traditional, intertwined areas. They are:

- Secrecy
- Authentication
- Non-repudiation
- Integrity control

Network Security in Wireless Systems

- **Secrecy (or confidentiality or privacy):**
  - Keeping information out of the hands of unauthorized users.
- **Authentication:**
  - Making sure that one is communicating with the intended person.
- **Non-repudiation:**
  - Using signatures and ensuring that a person cannot go back on his/her earlier communication.
- **Integrity control:**
  - Ensuring that the received message was not tampered with.

Security threats to wireless networks

- **Accidental attack:**

This gives rise to exposure due to frequent failure of devices and components because of their small sizes and capabilities.

Security threats to wireless networks

- **Passive attack:**
  - The goal of the intruder is only to monitor or get information that is being transmitted.
  - Attacks may include releasing message content or traffic characteristics.
  - Since no data are altered, passive attacks are difficult to detect.

Security threats to wireless networks

- **Active attack:**
  - In this type of attack, modifications of data or false data transmission takes place.
  - Man in the middle attack giving rise to masquerade or replay.
  - Denial of service (Dos) is possible where there is either temporary prevention of communication facilities or disruption of the entire network.

    This is done by boating it with a large number of messages to degrade the performance of the system.

Security threats to wireless networks

- **Unauthorized usage:**
  - This attack takes place because of the growing use of the Internet, which leaves the network vulnerable to hackers, viruses and intruders.
  - It can be presented by using proper user authentication techniques.

Security threats to wireless networks

- **Broadcast based:**

As mentioned earlier, an eavesdropper is able to tap the communication into the wireless communication channels, by positioning itself within transmission range.

Security threats to wireless networks

- **Device vulnerability:**

Mobile devices can be hijacked easily, and it secret IDs or codes are embedded in the device hackers may get access to private information stored on it and to other network resources.

Security threats to wireless networks

- **Heterogeneity:**

Mobile nodes need to adjust to potentially different physical communication protocols as they move to different locations.

Security threats to wireless networks

- **Resource depletion/ exhaustion:**

In mobile systems, resources like processing power and battery life are very limited. Hence, techniques such as public key cryptography cannot be used during normal operations to conserve power.

The device may also be left open to an attack that reduces the normal lifespans of the battery.

  - A DoS attack may consume and waste all the power in the battery leaving the unit unable to function.
  - In ad hoc networks, these attacks can cause routing nodes in the network to fall, making the network partially unreachable.

Security threats to wireless networks

- **Detectability:**

Mobile systems used in the military do not want to be detected. Even if strong encryption is being used and the data cannot be deciphered, just detecting the signal puts the mobile user at risk if its position can he located. The device can be jammed by local radio frequency (RF) interference or the user attacked.

Security threats to wireless networks

- **Theft of service:**

It is very easy to install, wireless LANs by just taking them ‘out of the box’ and by plugging them into the network so that they work.

In such systems, security settings are either disabled by default or factory-set default passwords are commonly known.

Unauthorized, nearby users, malicious or otherwise, can get a dynamically assigned Internet protocol(IP) address and connect to the internet.

Security threats to wireless networks

- **War driving/walking**:

This is like the popular war game called war dialing, which was an earlier technique for searching phone numbers with moderns attached to them.

As wireless LANs gain popularity, hackers can find them by just taking a notebook computer or pocket PC fitted with a wireless card and some detection software like netstumbler, kismet, airsort, etc. , an optional global positioning system (GPS) and driving/walking and the city. This information is then used to build a network from the identified Aps.