3

Security Features in Wireless Environment

3.1 Introduction

Security is a critical issue in mobile radio applications both for the users and providers of such systems. Although the same may be said of all communications systems, mobile applications have special requirements and vulnerabilities, and are therefore of special concern. Wireless networks share many common characteristics with traditional wire-line networks such as public switch telephone/data networks, and therefore, many security issues with the wire-line networks also apply to the wireless environment. Wireless networks, while providing many benefits over their wired counterparts, including the elimination of cabling costs and increased user mobility, present some serious security concerns. Unlike wired networks, where the physical transmission medium can be secured, wireless networks use the air as a transmission medium. This allows easy access to transmitted data by potential eavesdroppers. The mobility of wireless networks also introduces problems. The mobility of users, the transmission of signals through the open-air and the low power consumption of the mobile user bring to a wireless network a large number of features distinctively different from those seen in a wire-line

network. Issues of security and privacy become more prominent with wireless networks.

3.2 Mobile Network Environment

A simple mobile environment is shown in Figure 3.1.

Generally the following components are found in the mobile network environment:

- Mobile station (MS): A mobile terminal or mobile station is the equipment used by a client to obtain service from the mobile network. If he is within the coverage range of his mobile service provider, he can connect to the mobile network through the cell antenna using his mobile terminal.
- Cell antenna: Cell antennas provide network service facility within its coverage range to the mobile stations.
- Base station controller (BSC): Base station controller is commonly known as base station. It controls a cluster of cell antennas, and is responsible for setting up calls with the mobile station. Also, when the mobile station moves from

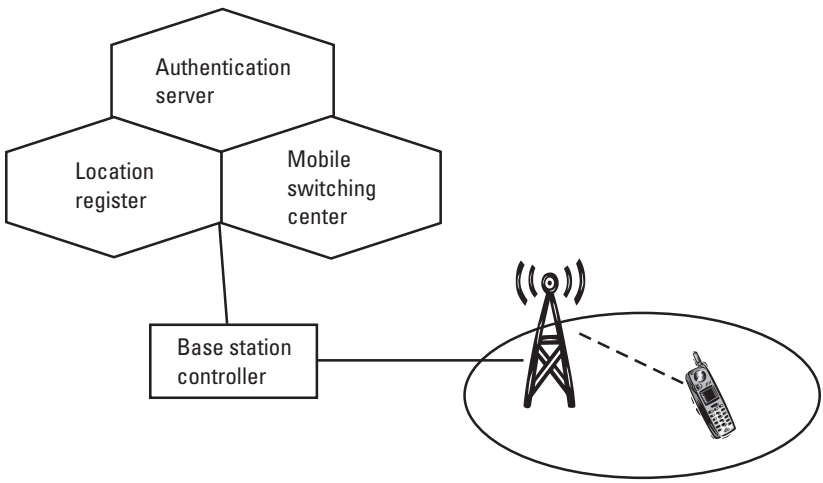

Figure 3.1 Mobile network.

one cell antenna coverage area to another, the base station manages the handoff process to maintain the continuity of the call. The hand off process is transparent to the mobile user.

- Mobile switching center (MSC): An MSC connects all base stations and passes messages and communication signals to and from mobile stations operating on the network.
- Location register: The location register contains information related to the location and the subscription of the users in its domain.
- Authentication server: An authentication server is present in every domain, and stores all confidential information, such as keys, and is assumed to be physically protected.

BSC, MSC, location register, authentication server – all these components of a mobile network can be integrally considered as domain servers. If a mobile station registers with a server, then the server in question becomes its home server and the network belonging to the home server is the home network. The domain administered by the home server is called the home domain. The mobile station can move from one place to another within the home domain or move outside its home domain to a "visiting" domain. The serving network is the one that is currently providing service in the area where the user has roamed. Typically, a serving network has to query the user's home network for information about the user for security and authentication purpose.

Mobile entities use air interface to communicate with the server in order to obtain the services as shown in Figure 3.2. The air interface is vulnerable to both active and passive attacks. An active attacker can subvert the communications between the communicating honest entities by injecting, deleting, altering, or replaying messages. A passive attacker can eavesdrop on the communication link to acquire knowledge of the communications.

The wireless medium is intrinsically a broadcast-based medium. An eavesdropper is able to tap into the wireless communications channels by positioning himself anywhere within the area of the cell.

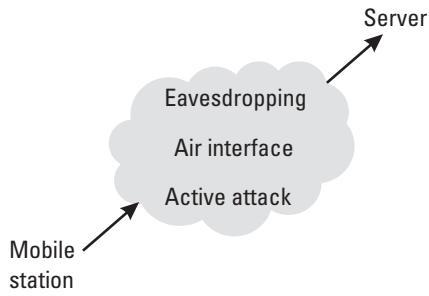

Figure 3.2 Mobile environment.

Since all transmitted data travel directly between a mobile host and the base station, it is possible to copy all the data of a particular message transmitted through the air.

It is also harder to control visiting hosts overloading the network with excessive transmissions, resulting in a sudden decrease in network performance. This may lead to denial of service to other mobile hosts because of the congested network.

There is a security threat during channel setup. When a mobile host "pops-up" in a cell, the base station (or any other network entity carrying out network management tasks and has jurisdiction over that cell) needs to update information on the network in order to allow messages to be routed to that mobile host correctly. This means that information on the physical location of the mobile host are available to entities that are able to see this routing information, an undesirable situation if that mobile user prefers to keep the location private. An impostor may also able to monitor that mobile user and begin connecting to the network using that mobile user's identity after a disconnection. The impostor will then have access to all the resources that are available to the real user. The real user may even be denied connection later because the base station might think that it is trying to reconnect again for the second time.

3.3 General Security Threats of a Network

A network environment is, in general, susceptible to a number of security threats. These include the following:

Masquerading By masquerading, an entity can obtain unauthorized privileges. In a network system, a masquerading user or host may deceive the receiver about its real identity.

Unauthorized Use of Resources The unauthorized user can access the network system and utilize the resources for its own purpose.

Unauthorized Disclosure and Flow of Information This threat involves unauthorized disclosure and illegal flow of information stored, processed, or transferred in a network system both internal and external to the user organizations.

Unauthorized Alteration of Resources and Information Unauthorized alteration of information may occur both within a system and over the network. This attack may be used in combination with other attacks, such as a replay, whereby a message or part of a message is repeated intentionally to produce an unauthorized effect. This threat may also involve unauthorized introduction, including removal of resources from or into a distribution system.

Repudiation of Actions This is a threat against accountability in organizations. For instance, a repudiation attack can occur whereby the sender (or the receiver) of a message denies having send (or received) the information.

Unauthorized Denial of Service Here the attacker acts to deny resources or services to entities authorized to use them. In the case of a network, the attack may involve blocking access to the network by continuous deletion or generation of messages, causing the target to be either depleted or saturated with meaningless messages.

3.4 Limitations of Mobile Environment

Mobile devices are designed to be portable (i.e., light and small). Until a more suitable alternative is found, mobile devices will more than likely continue to be battery powered in the foreseeable future. The power consumption of mobile devices directly affects their usage time. In order to conserve energy, both processing speeds and processor cycles need to be reduced. Because data transmission also

consumes energy, it, too, should be reduced. The former imposes limits on the computational complexity of the encryption algorithms and the number of messages involved in security protocols. In addition, integration of security features into mobile devices must take into account applicable restrictions such as small packet size, low bandwidth, high transmission costs, limited processing and storage resources, and real time constraints.

3.5 Mobility and Security

The mobile environment aggravates some of the above security concerns and threats because the security of wireless communication can be compromised much more easily than that of wired communication.

The situation gets further complicated if the users are allowed to cross security domains. (For details on domain boundary crossing, see Section 3.7.4.)

Being reachable at any location at any time creates greater concern about privacy issues among the potential users. For instance, there may be a need for developing profiles that specify who, when, and from is authorized to get a service.

Mobile users will use resources at various locations, provided by various service providers. It is important to understand the trust issues involved when mobile clients are allowed to use resources of different servers at different locations.

Integrity and confidentiality of information stored on the mobile appliance is another important concern. Needless to say, user anonymity [1] is important in a mobile environment. Different degrees of anonymity can be provided, such as hiding user identity from eavesdroppers or from certain administrative authorities.

3.6 Attacks in Mobile Environment

Many ingenious attacks have been developed for compromising security protocols. The results of these attacks, if successful, can range from a mild inconvenience to a severe breach of security. Even when the attacks are unsuccessful they can consume the processing

resources of the attacked party and thus reduce the resources available to legitimate communication.

A general problem with wireless communications is that attacks broadcast over the network are difficult to prevent. In a wired network, the attacker must physically "tap" into a wire in the network. Standard security measures can be taken to reduce the access to network wires, such as restricted building access or locked communication closet, and upon detecting and locating a tap, it can be easily removed.

This same property does not exist in a wireless network. Any party that possesses the proper equipment, whether a legitimate member of the network or not, can receive and send messages in the network. When the attackers are discovered it is difficult to purge them from the network because they can roam freely throughout the wireless region while attacking at will.

The attacks described in the following sections are particularly troublesome in wireless communications because they are easy to execute yet impose significant overhead on user or the wireless network. Remedies for each of these attacks are also discussed.

3.6.1 Nuisance Attack

The primary concern of security protocol is to successfully defend against all forms of attacks. However, even when an attack is thwarted, it has typically required the entity or the server to expend processing and communication resources to discover the attack. These attacks are referred to as nuisance attacks, because while they cannot compromise security, they can disrupt the activities of legitimate users. This disruption can cause significant problems in a wireless network since the mobile terminal typically consists of minimal processing resources. Therefore, the resulting attacks can severely affect the mobile principal's ability to conduct legitimate communications. Of greater concern are the communications bandwidth and cost. A nuisance attack introduced into a wireless network can result in several unnecessary wireless responses being expended before the attacking message is discovered to be fraudulent. Protocol design should try to minimize the possibility or at least the impact of the nuisance attack.

3.6.2 Impersonation Attack

By impersonating a legitimate user, the attacker will try to eliminate one of the communicating parties from the intended communication, making the other communicating party believe that he is legitimate. The attacker can impersonate the mobile entity and with a high computational ability, it can also impersonate the server. In order to avoid impersonation attack, the protocol design should consider the mutual authentication of the legitimate entity and the server.

3.6.3 Interception Attack

In wireless communication, communicating messages are transmitted by air, allowing someone to easily tap into the communication without being detected, and access all communicating messages. In a wireless environment, it is not possible to eliminate interception attack, but by encrypting all the messages in communication, it is possible to prevent the attacker from gaining any valuable information.

3.6.4 Replay Attack

Using this method, the attacker intercepts and stores all communications between the communicating parties. At a later time, the attacker impersonates one of the communicating parties by replaying the stored messages. By incorporating the session variant parameter in authentication messages, it is possible to resist replay attacks.

3.6.5 Parallel Session Attack

Using this attack method, the attacker begins communication with one of the communicating parties and uses it as an oracle to compute the session key. This method is most successful when the flow of messages between the communicating parties is of the same structure. These attacks can be effectively prevented by maintaining asymmetry in the back and forth messages and by including direction dependent parameters in the message flows.

Bird et al. [2] identified another form of oracle attack, one in which an adversary starts two separate authentications sessions with the server and user. When interacting with the server, it becomes the

user, and vice versa. It tries to take the advantage of the messages from the authentication session with the server to impersonate the server in authentication session with the user. This kind of attack can be effectively prevented if the encrypted messages used in each run of the protocol are different from, or logically linked, with one another.

3.7 Security Issues in Mobile Environment

In the following sections, four major areas of mobile systems security are discussed, namely *authentication*, *anonymity*, *device vulnerability*, and *domain crossing*.

3.7.1 Authentication

The primary objective of an authentication scheme is to prevent unauthorized users from gaining access to a protected system [3]. As with current distributed systems, authentication is a necessary procedure for verifying both an entity's identity and authority. The level of trust for a particular entity depends on the outcome of this authentication process. Ideally, user authentication should be carried out transparently, without disruption to whatever the user's current task. Authentication protects the service provider from unauthorized intrusion. By mutual authentication [4] mobile station also authenticates the server. There are two reasons why this could be of importance. First, it prevents a malicious station from pretending to be a base station. Then it permits the MS to choose the services of a particular base station in the presence of colocated networks.

In practice, most authentication protocols require the home *authentication authority* (or authentication server) to be contacted during or before the execution of the protocol. Consider the overhead that will be incurred when this has to be done for many mobile users entering the foreign domain. Furthermore, the "transparency" requirement for authentication protocols would be difficult to meet. The completion time for each protocol also depends on the quality of the link between the visited domain and the mobile user's home authentication server. This also means that the home authentication server must be available at all times. These last two factors, the link quality between the visited domain and the user's home

authentication server and the availability of the authentication server itself, are unpredictable and therefore cannot be guaranteed.

While the use of certificates may relax the requirement of contacting the user's home authentication server, it also contains some undesirable properties. For one, it is irrational to assume that the certifying authority signing the certificate is globally and unconditionally trusted by every entity. Also, a mobile user may travel from one domain to other domains and it may not always be preplanned. In these instances, it is not possible for the user to obtain certificates issued by his home domain for the all other domains he might visit and the visiting domain authority may not accept the certificate.

Another problem is that certificates do not reflect the *current status* of its owner/carrier (e.g., the current balance of a bank account or a record of his or her behavior in previously visited domains). It is difficult to embed some information about the current status of the user into the certificate by the server and at the same time be sure that the user cannot alter that information or present only certificates that provide the most positive credentials. Revocation of certificates will also become a more difficult problem, and one concerned with scalability, in that mobile users move frequently, and their locations could be anywhere in the world.

Engineering good authentication protocols for mobile systems carry an extra burden of anonymity requirements. It is imperative that authentication protocols release as little information as possible relating to the principals involved in the protocol execution.

3.7.2 Anonymity

Anonymity is the state of being not identifiable within a set of principles [5]. Information about a particular person or organization is private and should only be known to its owner and to whomever he grants access rights. Privacy should be preserved in any kind of information system, be it fixed or mobile. The type of information that a user may want to keep private could include his real user identity when on-line, his activities, his current location and his movement patterns. Preserving anonymity [1] is of greater concern in mobile systems for several reasons. Mobile systems yield more easily to eavesdropping and tapping, compared to fixed networks, making it easier

to tap into communication channels and obtain user information. As users move around, a new kind of information immediately becomes valuable, such as detailed information about the movement and location of the user. This may also provide clues to any user interaction at a given point in time. Users will also move in and out of foreign domains without the prior knowledge of the user, and therefore may not be completely trustworthy. Moving across foreign domains thus results in increased risk to user information. Current network implementers of mobile communication systems store a lot of user related information on network databases, especially for mobile telecommunication networks. This is done to assist in user mobility support as well as billing and authentication. This makes the user information more widespread and highly available. It is also uncertain whether the environment where this data is stored is safe and trustworthy. The following issues should be considered to solve the anonymity problem:

- Preventing other parties from making any association of the user with messages that he or she sent or received;
- Preventing any association of the user with communication sessions in which he or she may participate;
- Preserving the privacy of location and movement information of users;
- Preventing the disclosure of the relationship between a user and his or her home domain;
- Preventing any association of the user with the foreign domains he or she may have visited;
- Disallowing the exposure of a user's activities, by hiding his or her relationship with the visited domains.

Users can be denied service by various mechanisms, usually by either "cutting off" the communication channel between the client and the server or by flooding the network to the extent that no more bandwidth is available for use, rendering the network effectively nonoperational. With *unselective* denial of service, whole services or large parts of a network are disabled (e.g., using explosives), and these

are usually detectable. *Selective* denial is less evident and its victims are usually well defined (e.g., a particular client on the network). Anonymity is an obvious solution to the latter problem.

A common solution that has been adopted, providing a certain degree of anonymity in current systems, is by means of an *alias,* or a temporary identity. Aliases or nicknames allow a user to be referenced without revealing his real identity. Another way to provide user anonymity is to encrypt the real identity [6].

3.7.3 Device Vulnerability

Mobile devices are designed to be small and lightweight, making them highly portable. These features of mobile devices make them potentially vulnerable to being misplaced or lost, and worse, to theft. Even though losing the physical device itself is an unsatisfactory enough outcome, a more detrimental consequence is the owner's deprivation of the information or data that is (or was) contained in his or her device. Hardware can be repurchased, but information, especially the kind that is updated frequently, cannot be refabricated that easily. Worse still, some of the data may contain a secret not even known to the owner.

Mobile devices may also be used as a control device. Examples include active badges for controlling access to workstations and building entrances and even devices used when purchasing goods or withdrawing money (e-cash) from an ATM. Without these devices, the users will be denied access to most of these facilities and services. Furthermore, if procedures for obtaining a replacement device of this type take time to process, the device owner's industrial and social progress will be severely affected.

If the device is stolen, thieves who can disarm the safety features on the device can then access the private information contained within. The thief may also get unauthorized access to services that are available via that device, prior to the theft being discovered and privileges are revoked.

3.7.4 Domain Boundary Crossing

A security domain means a set of network entities on which a single security policy is employed by a single administrative authority.

Security domain boundaries are crossed when a mobile user leaves one security domain and enters another.

Upon entering a new domain, the trustworthiness of the new domain environment has to be ascertained by the mobile user, and vice versa. This is usually carried out using mutual authentication protocols where two entities mutually authenticate each other during one protocol execution. It is important at this stage to determine the *trustworthiness* of the domain and user. The level of trust established will form the basis on which security related activities and decisions are made.

Another important motivation for domains to screen its visiting hosts is to uphold its image as a *safe* domain. Much like geographic domains (e.g., cities or suburbs), a hostile environment will tend to be avoided and its resident occupants would want to migrate to a safer haven. The consequences would lay the economical soundness of that domain, among other activities, in jeopardy.

References

[1] Samfat, D., R. Molve, and N. Asokan, "Untreacibility in Mobile Networks," *Proc. of ACM Int. Conf. on Mobile Computing and Networking,* Berkeley, CA, November 1995.

[2] Bird, R., et al., "Systematic Design of a Family of Attack-Resistant Authentication Protocols," *IEEE Journal on Selected Areas in Communications*, Vol. 11, No. 5, 1993, pp. 679–693.

[3] Morris, R., and K. Thompson, "Password Security: A Case History," *Communications of the ACM*, Vol. 22, No. 11, 1997, pp. 594–597.

[4] Joos, R. R., and A. R. Tripathi, *Mutual Authentication in Wireless Networks,* Technical Report, Computer Science Department, University of Minnesota, 1997.

[5] Pitzmann, A., and M. Köhntopp, "Anonymity, Unobservability, and Pseudonymity—A Proposal for Terminology," *Designing Privacy Enhancing Technologies, LNCS 2009*, Springer-Verlag, 2001, pp. 1–9.

[6] Park, C. S., "Authentication Protocol Providing User Anonymity and Untreacibility in Wireless Mobile Communications Systems," http://www.misecurity.com/ko/forum/ forum_06.pdf.