2011 International Conference on Network and Electronics Engineering
IPCSIT vol.11 (2011) © (2011) IACSIT Press, Singapore

Security Threats for Widespread Services in Mobile Environment

Hassan Shahba and Masoud Sabaei

Computer Eng. and Information Technology Dept.
Amirkabir University of Technology, Tehran, Iran
E-mail: Hassan.shahba@aut.ac.ir, Sabaei@aut.ac.ir

Abstract. Recently mobile widespread services are widely deployed. The delivery of these services should be secured. In widespread mobile environment, various security threats are posed to the user, network and service/content providers, so security requirements are needed to be identified to reduce these threats. In this paper these threats, their possible solutions, and open issues are studied.

Keywords: Security; Mobile; Widespread; HMIPv6

1. Introduction

Dreams of mobile widespread services are quickly becoming a reality. These services are applicable for any wireless network access technology (such as: Bluetooth, WIFI, WIMAX, UWB). As you see in Figure 1, there are three important perspectives in the mobile widespread services environment [1]:

1-User
2-Network
3-Service/content provider

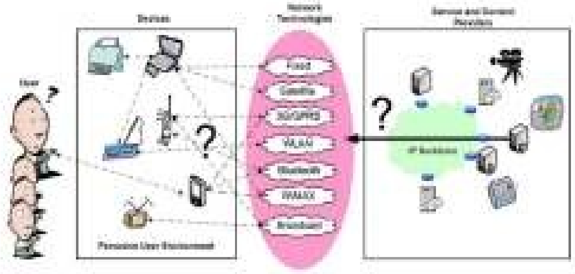

Fig.1- A mobile widespread environment [15].

1.1. User Perspective

From the user perspective, the basic need of the user is providing easy access to the proper services. The Internet, today, includes widespread heterogeneous networks with different capacities (bandwidth, interface speed, delay and edge to edge connection). Also the use of laptops, Palmtops, mobile and different operating systems are continuing in today’s systems. All these differences with the high volume of information of different services create a lot of

Complexity. In these networks security against threats and privacy for users are the biggest challenges.

1.2. Network Perspective

From the network perspective providing security, service quality and transitioning in different participating networks is a key factor in preparing an acceptable level of feedback. Heterogeneity in network security, quality service, transmission management, is causing a lot of complexity. A network framework to collect this information together is needed in the network.

1.3. Service Provider Perspective

From the content and service providers, multi-network operation companies promise a possible new series 'widespread services', such as context aware services. In this view, the security is very important to protect the interests of the service/content provider from malicious users and other enemies.

2. Security Threats

In this section we separately study the security threats from all three perspectives of the mobile environment (user perspective, network perspective, service/content providers perspective).

2.1. User Perspective

- *Spoofing:* A malicious entity may disguise as a provider of legal services/contents with the aim of luring a user to have a bogus interaction of services with him.
- *Information Disclosure:* A users personal identifiable information (such as: identity, credit card information, individual and location information ...) may be disclosed for a service/content provider or an eavesdropper while having contact with the service/content provider. Outcome of this threat is loss of user privacy or surrendering to threats of identifying theft.
- *Profiling:* From prior service interactions that a user has had with a service provider, the Service/Content Provider may be able to learn valuable information about the user (e.g. age, gender, income, habits, spending patterns, and etc.), and build up a profile of the user. This may be used for future marketing purposes, including targeted pricing or targeted marketing. This threat may compromise a user's privacy.
- *Profile Linking:* service/content providers may collude, and exchange profiles with each other and may exchange the interactions and activities of the members to build a more complete profile. Again, this information may be used for the future user's behavior and it may endanger the privacy of the user.
- *Framing:* different types of content distribution protection (CDP) (e.g. watermarking, fingerprinting, and etc.) and digital rights management (DRM) mechanisms are employed by content providers to deter and prevent content users from illegally distributing copyrighted content. Most of the existing CDP or DRM solutions do not protect an honest content user from being accused (or framed) by a content provider of illegal content distribution.
- *Information over Loading:* The user may face a tremendous amount of service information (as an advertisement service) of the future service providers or spam senders. These may lead to the following threats:
    - *Denial of Service:* the user's device may be the overflow of advertising services (both legal and illegal) and that this may prevent proper communication between the user and service provider.
    - *Service Selection Dilemma:* It is quite likely that the specific service is being offered by different providers. In this case the user has a lot of options and all of them enjoy the same priority, a user may not be in a position to select the best service.
- *Configuration Complexity*
    - *Device and Application Settings:* User can have different types of devices (e.g. laptop, PDA, cell phone, iPod, etc.). Different devices may be used to access different services depending on the situation/context, physical location of the user, language, or services that he intends to use. Before the service can be used, first the device should appropriately be configured and set up. For a non-expert user, this can be very difficult and daunting task. A wrongly configured device may even pose a security threat/risk to both the user and the service providers.
    - *Security Parameters:* Often, users select a password that is easy to remember. These passwords are usually weak. Moreover, for simplicity and usability, users may set the same usernames, passwords/pins for different applications and services that they use. So users' passwords can be easily guessed, and the end user's security can be seriously compromised.

2.2. Network Perspective

Application level security is not always guaranteed. Network security threats are generally divided into two categories: Active Threats and Passive Threats. Each is subdivided into other threats [2].

- *Passive Threats:* A *passive* threat is a threat in which unauthorized users could access information but not change them and can only eavesdrop. This type of threat is divided into two categories: traffic analysis, eavesdropping.
    - *Eavesdropping:* the adversary may monitor transmission for message content at the network level (e.g. tuning into the data transmissions between wireless handsets and base station).
    - *Traffic Analysis:* The adversary, in a more subtle way, may gain intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is available in the flow of messages between communicating parties.
- *Active Threats:* In this threat an adversary makes modifications to a message, data stream, or a file. Active threats include: masquerading, reply, distribution, message modification, and denial of service. These threats are described below:
    - *Masquerading:* the adversary may impersonate as an authorized user and then gain access to unauthorized information.
    - *Replay:* the adversary may listen to the message (eavesdrop the message) and then send it to the end user as an authorized sender.
    - *Message Modification:* the adversary may delete, add, change or reorder the message.
    - *Denial of Service:* In this threat the adversary may disrupt the service access.

2.3. Service/Content Provider Perspective

- *Spoofing:* A malicious entity may also masquerade as a legitimate user and interact with a Service/Content Provider.
- *Illegal content distribution:* Illegal distribution of site's contents (e.g., music, movies ...) is a great challenge for the digital content industries. This directly translates to loss of revenue for content providers. The mobile and dynamic nature of a widespread environment actually makes it easier to distribute/share illegal content.
- *Rogue behavior:* privacy enhancing technology may be used by users to protect their privacy and identities, when they are interacting with service/content providers. If these users misbehave (e.g. distribute site contents), service providers will be able to trace or black list these members, and then decide the next course of action (e.g. prosecuting them).

3. Security Requirement

3.1. General Security Requirement [3]

- *Confidentiality:* Confidential information that has made property is not available or disclosed to unauthorized persons, institutions, processes, or in other words, each system entity is unauthorized.
- *Integrity:* Integrity is the property that data have not been changed, destroyed, or lost in an unauthorized or accidental manner. It deals with consistency of and confidence in data values, not with the information that the values represent.
- *Authentication:* Authentication is the process of verifying an identity claimed by or for a system entity. Output process consists of two phases: the identification stage to provide ID to security systems and Confirm step that information or the production and prove out the connection between institutions and ID.
- *Authorization:* Permission or the right that is granted to a system entity to access a system resource. "Authorization process" is a method for granting such rights. To "authorize" means to grant such right or permission.
- *Non-repudiation:* non-repudiation service provides security against the false denial of involvement in an action. Non-repudiation does not and cannot prevent an entity from repudiating an action. Instead, the service can be stored and later presented to a third party to resolve disputes that arise if an action is

repudiated by one of the entities involved.

3.2. Specific user needs and security service providers

- *Secure service selection/recommendation:* When more than one provider offers you a type of service a selection/recommendation mechanism may be used by a user for decision making process. The selection mechanism may take the users preferences, habits and the context information as input.
- *Secure zero configurations:* device settings or user network configuration may automatically be configured on behalf of a user to a process through a process called zero configurations; this process should be secured [4].
- *Secure service discovery:* Before you can run a service between user and service provider, you must run a service called service discovery, service provider should run this service to understand what kind of service does user need. This action must be safe because someone malicious can find user required service through eavesdropping.
- *Privacy and anonymity*- Users are becoming increasingly concerned about their (online) privacy while transacting online or digitally.
- *Content distribution protection (CDP)*- Service providers may employ content distribution protection mechanisms to prevent or deter users from illegally distributing copyrighted content to other people [15].
- *Secure service provision* - The delivery of a service to the end user is known as service provision. It is imperative that this process is secured to guarantee the correct service is indeed being delivered to the intended recipient.

3.3. Specific Network Security Requirement

- *Network access control* - Access control makes sure that the unauthorized users are denied network access, while the legitimate users are granted the network access that they are authorized to use. The MN needs to be authenticated and authorized before it can enter the access network [15].
- *Availability* - Availability ensures that network resources/services, are available and protected against attacks.
- *Network Infrastructure Protection* -Network Infrastructures (routers and servers) should be protected against potential attacks [15].
- *Location privacy* - For certain services, it may be important to have user location privacy [15].
- *Routing anonymity:* anonymous routing layer network may be used, to end points to prevent communication (sender and receiver) from being linked.
- *Optimization of Security, QoS and Mobility Management:* Security (Sec) QoS management and transactions (Trans) should be integrated in the network perspective. In order to optimize (sec, QoS, mob) compound, Mobile IPv6 may be used, to display the correct mobility IPv6. The integration problem is easy to optimize (Sec and QoS) in mobile environment page IPv6. When the security infrastructure Mobile IPv6 is made, inter cooperation with QoS issues must be taken into consideration. For example, the QoS framework can be reliable for transportation security messages [15].
- *Secure multicast provisioning in the mobile widespread networks:* In the case of multicast traffic, the potential of attacks is even greater than for unicast traffic because of the inherent broad scope of a multicast session. In order to create a private multicast session, access to the required session keying material should be restricted through a registration and authentication process. Only authorized users are able to gain access to group keying material and to subsequently participate in the session.

4. Possible Solution

4.1. IPSec recall and AAA and Hierarchical Mobile IPv6

The Integration of IPSec/AAA and Hierarchical Mobile IPv6 solution is fully integrated, IPSec may be used to secure the data traffic in the network, and AAA may be used to authenticate the mobile node used to access the network. The protocols which are able to enhance mobile IPv6 (MIPv6) for faster handover are expected to be widely deployed. HMIPv6 is one of these proposals. Hierarchical Mobile IP (HMIP) as an extension to

Mobile IP adds a strategic node Mobility Anchor Point (MAP) to the set of network elements. The MAP can be placed in any level of hierarchical structure of the network, and should serve an optimized number of subnets [5]. The goal in domain oriented Mobility Management schemes like HMIP is to limit the signaling messages locally within the region. This is due to the fact that binding updates (BD) are sent from Mobile Node (MN) directly to MAP rather than Home Agent (HA).

This means that MN's exact position is hidden from the outer region. Thus the signaling messages in macro-level get reduced as long as the "Mobile Node" stays in a specific region. In such a structure, the MN has two "Care-of-Addresses" (CoA). The MN registers the obtained address from its serving "Access Router" (AR) with the MAP.

- *From the data traffic point of view* - MAP is acting as the "anchor point" for all the data traffic, which means that the IPv6 traffic are transmitted either from the MN to the Correspondent Node (CN) or from the CN to the MN through MAP. The data traffic should be protected to overcome existing network security threats. The IPSec protocol suite, which will be explained in greater detail in the next section, may be used here to secure the data traffic in HMIPv6 [15].
- *From the signaling point of view* - the authenticated access for IPv6 mobility should be available in the HMIPv6 scenario. It basically means authenticating the MN in order to grant network access. AAA protocols, which will be explained in greater detail in the following section, can be used to achieve this goal. In HMIPv6, MAP is an anchor point not only for the data traffic, but also for all of the signaling information. Therefore, if AAA protocols are used to provide the authenticated access, MAP will be a natural choice to act as the AAA client that is responsible for initiating AAA request and transmitting all of the authentication information to the AAA server in the MN's home domain. In other words, MAP is acting as the anchor point in HMIPv6 to exchange the authentication information between the foreign domain and the home domain [6].

1) IPsec

IPSec, an IP layer protocol suite, enables the sending and receiving of cryptographically protected packets of any kind (TCP, UDP, ICMP, etc.) without any modification. IPSec provides two types of cryptographic service[8]. IPSec can provide confidentiality and authenticity, or it can provide authenticity only by following two protocols: ESP (Encapsulated Security Payload), which is defined in the RFC 4303 [7]. and AH (Authentication Header) which is defined in RFC 4302 [9].

2) AAA: Authentication, Authorization, Accounting

Authentication involves validating the end user identities before granting them access to the network [10]. This process is based on the fact that the end user processes a unique piece of information 'username/password combination, a secret key, and perhaps biometric data like (fingerprints) that serves as unambiguous identification credentials.(Figure 2)

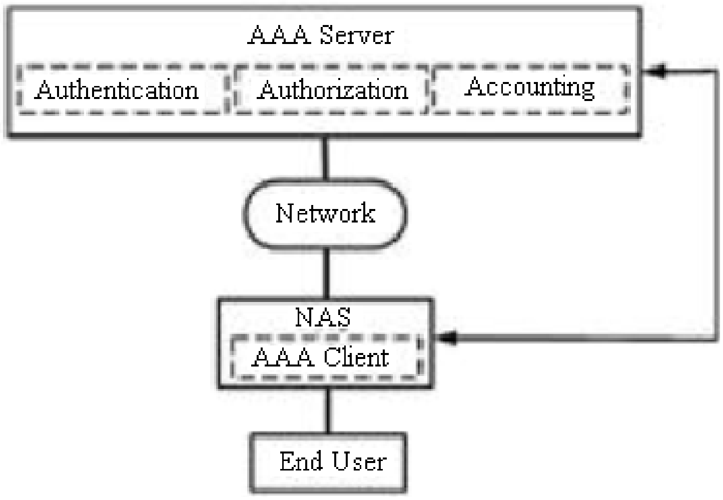

Fig.2-The fundamental components of AAA [15].

5. Open Issues

5.1. Privacy (anonymity)

Authentication is an important need for security and is usually used for the users' identity authentication for a service provider. On the other hand, the users and consumers are extremely concerned about protecting their privacy, thus they may prefer to interact with service providers anonymously (or pseudonymously), and in such circumstances the authentication of the users' identity may be undesirable.

Therefore to protect the privacy of a user, other attributes of the user may need to be authenticated to the service providers. If the privacy is preserved by anonymity of users how can a service provider be convinced that a particular user is trustworthy? Therefore, authentication and privacy do not correspond with each other.

5.2. Problem within the mobile IPv6 and IPSec

Mobile IPv6 integration with IPSec is not yet well achieved. IPSec specifications do not work properly with mobility schemes based on addresses. RFC 3776 [11] explains how IPSec is used with Mobile IPv6 to protect the signaling messages. Since IPSec architecture is revised in 4301 [7] RFC some progresses has been made in RFC 4877 [12] for the Home Agent and Mobile Node in order to use the IPSec architecture and revised IKEv2. In RFC 4877 [12], IPSec is used to protect return routability signaling or payload packets. The issues related to address changing are still very complicated. For example, when the mobile node CoA changes as a result of an accepted BU, special treatment is required for the next packets sent using the previous security association. And Home Agent should set a new CoA as destination address for packets. Such address changes can be implemented in RFC 4877 [12] by introducing an API from MIPv6 implementation to the IPSec implementation. But this is just limited to the cases based on BU received by the Home Agent. Address changes based on other sources such as the BU to the CN protected by return routability, may still lead to security vulnerabilities. Therefore, IPSec and MIPv6 integration is an open issue in terms of the addresses [15].

5.3. Secure Multicasting for Widespread Mobile Services

For secure multicasting, a multicast capable implementation of IPSec is necessary to be used by the receivers [14]. The secure multicast and key management architecture are defined by the MSEC group in IETF in RFC 3740 [15] and RFC 4046 [15]. In addition, for multicasting in large scales efficient key distribution is required, like using a Logical Key Hierarchy (LKH). LKH is a mechanism for security key management in a group of entities, providing the ability of initializing a common key and then to rekey the group as required. Such architecture does not address Mobility issues. Therefore the interaction between Multicast Key Management and mobility management is an open issue. Thus there is a need for coordinate key tree structure and key delivery (routing) to the mobile host. This issue is even more complicated if there are QoS provisioning for such groups [15].

5.4. Security -QoS-Mobility Management Optimization

Increased Security mechanisms, such as providing encryption, will affect the usage of resources. Increased mobility management mechanisms like high paging and routing update will also affect usage of resources. At the same time, providing high QoS may also affect the resource allocation. Thus, different balance points must be found in the different scenarios as known under the definition of network policy. Due to limited system resources, conflicts between security management, QoS and mobility always exist. Defining an Optimization point becomes important and remains a challenge.

5.5. Problem with AAA key distribution scheme in Mobile IPv6

Registration key distribution scheme is based on AAA server in home domain (AAAH) that also plays the role of key distribution center. Since the message exchange between the AAA server and in the Home domain (AAAH) and AAA server in the foreign domain (AAAF) is necessary for each registration request initialized with the MN, it may have a delay more than one caused by the base mobile IP registration protocol. So a new key management scheme for securing Mobile IP registration is necessary to simplify the distribution of the registration key and reduces the delay associated with the AAA protocol, is required [13].

5.6. Problem with AAA and Hierarchical Mobile IPv6

It is proposed that the AAA infrastructure can be used in mobile IPv6. However, when the AAA is used in HMIPv6 some issues may arise. HMIPv6 provides MIPv6 with MAPs that can handle authentication and mobility management in visited networks. One potential problem is whether the hierarchy of MAPs is feasible. In addition, more considerations may be needed about how to use the AAA infrastructure for temporary security associations between mobile nodes and visited networks. Therefore, applications that require subsequent authentication may not need the signaling between the Home and the visited domain [15].

6. Conclusion

In widespread mobile environment, various security threats posed to the user, network and service/content providers were studied. Also a set of security requirements were identified to reduce these threats. Then some possible solutions were suggested and then had a discussion on various open issues which are not properly addressed by the current solutions.

What was done in this article showed that many security threats that are in widespread environment can occur in more than one perspective (user, network and service provider). Examples of such threat include: spoofing/Masquerading, information disclosure/eavesdropping, profiling/traffic analysis. However, different security solutions may be required to reduce these threats in each of the perspectives.

7. References

[1] Mobile VCE members, "Removing the harriers to ubiquitous services," Mobile VCE Document, 2003.

[2] T.Karygiannis and L.Owens, "Wireless network security: 802.11, Bluetooth and handheld devices," National institute of standards and technology special publication 800-48, November 2002.

[3] Shirey R. Internet security glossary. RFC2828; May2000.

[4] Yan E. Zero configuration networking. The Internet Protocol Journal 2002; 5(4): 20-6.

[5] H.Soliman, C.Castelluccia, K.ElMalki and L.Bellier, "Hierarchical Mobile IPv6 mobility management," Internet draft: draft-ietf- rnipshop4140bis-OO.txt, IETF, March 2007.

[6] Moloud Mousavi and Alejandro Quintero, "Selection mechanism in Hierarchical Mobile IP," IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMobapos), pp. 321 - 328, June 2006.

[7] Kent S. IP authentication header. RFC 4302; Dec. 2005.

[8] Hoffman P. Crypto graphic suites for IPsec. RFC 4308; Dec. 2005.

[9] Kent S. Extended Sequence Number (ESN) addendum to IPsec Domain Of Interpretation (DOI) for Internet security as sociation and Key Management Protocol (ISAKMP). RFC 4304; Dec. 2005.

[10] De Laat C, Gross G, Gommans L, Vollbrecht J, Spence D. Generic AAA architecture. RFC 2903; Aug. 2000.

[11] Arkko J, Devarapalli V, Dupont F. Using IPSec to protect Mobile IPv6 signaling between mobile nodes and home agents. RFC 3776; June 2004.

[12] Devarapalli V, Dupont F. Mobile IPv6 operation with IKEv2 and the revised IPSec architecture. RFC 4877; April 2007.

[13] Kang Hyun-Sun, Park Chang-Seop A key management scheme for secure Mobile IP registration based on AAA protocol. IEICE Trans. Fund. June 2006; E89-A(No.6).

[14] Holbrook H, Cain B. Source-specific multicast for IP. RFC 4607; Aug. 2006.

[15] Adrian Leung, Yingli Sheng, Haitham Cruickshank, The security challenges for mobile ubiquitous services, Information Security Technical Report, Volume 12, Issue 3, 2007, Pages 162-171