Mobile IP Security in VPNs

M. C. NICULESCU, Elena NICULESCU and I. RESCEANU
Dep. of Mechatronics and Electronics and Instrumentation
University of Craiova
Al. I. Cuza Street, No. 13, Craiova, RO-200585
ROMANIA

Abstract: -. This paper presents a survey of common security threats which mobile IP networks are exposed to as well as some proposed solutions to deal with such threats. In a typical RFID (Radio Frequency Identification) system, tags storing a unique identifier and additional data are attached to objects or issued to people. When a tag or a group of tags is placed in the radio frequency field of a reader, the data contained in the tag's memory can be accessed by the reader. The data are usually preprocessed and passed on to enterprise applications by the RFID middleware. The RFID system, consisting of readers and tags, along with the RFID middleware and the enterprise applications is referred to as the RFID infrastructure.

Key-Words: - Mobile IP, Security, Protocol, Networks, Key, Authentication, VPN.

1 Introduction

Whilst offering great flexibility and potential, mobility exposes mobile nodes and consequently entire networks to security threats that are not trivially solved. On the contrary, combat against such threats requires appropriate services and protocols. In this paper we present a survey of common security threats which nodes in mobile IP campus intranets and in the Internet are exposed to as well as the technologies, services and protocols that have been used to combat these threats.

The next section describes how security is dealt with general IP networks, providing the fundamentals for the following discussions. Mobile IP campus Intranets are discussed in Section 3. Section 4 extends the discussions to internet-wide mobile IP deployment. Finally, Section 5 presents some conclusions.

2 IP Security

A security service is a collection of mechanisms, procedures and other controls that are implemented to help to reduce the risk associated with a specific threat to a system.

For example identification and authentication services help to reduce the risk posed by access to the system by an unauthorized user or attacker. Logging or monitoring is a service that helps to detect security breaches. For a specific application some security services might be more important and some less. The most important security services are:

1. Confidentiality, which ensures that data, software and messages are not disclosed to unauthorized parties.
2. Integrity, which ensures that unauthorized parties do not modify data, software and messages.
3. Authentication, which ensures that a network can only be accessed by individuals that are authorized.
4. Nonrepudiation, which ensures that entities involved in a communication cannot deny having participated in it.
5. Availability, which ensures that a service is available at all times.
6. Access Control, which ensures that network resources are being used in an authorized manner.

Aiming at providing users with secure communications over the Internet, the Internet Engineering Task Force (IETF), under the IP Security Protocol Working Group, has defined the Security Architecture for the Internet Protocol [8]. Known as IPSec, this architecture defines a suite of protocols that describes security mechanisms and services for both IPv4 and IPv6 and upper layers1. IPSec is organized as shown in Fig. 1. Three primary protocols are defined: the Encapsulating Security Payload (ESP) [1], the Authentication Header (AH) [2] and the Internet Key Exchange (IKE) [7].

AH is used to provide integrity and authentication for IP datagrams and protection against replays. Integrity ensures that the datagram

was not altered in an unexpected or malicious manner. Authentication verifies the source's claimed identity. And replay-protection prevents users from receiving packets intentionally delayed by nodes with malicious intentions.

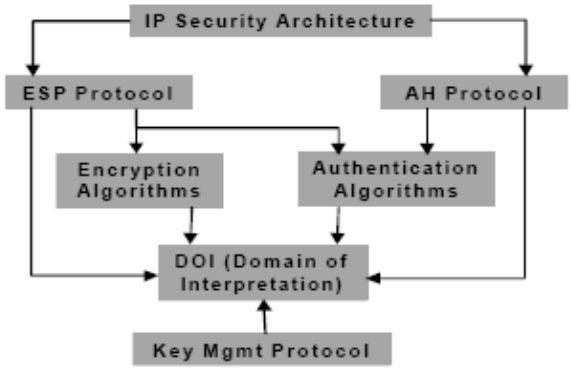

Fig. 1 IP Security [5]

The AH protocol is designed to work with many different authentication algorithms, whereas the most used is the mandatory Message Digest (MD) 5 [2]. MD5 is a one-way mathematical function that produces a 128-bit unique representation of the data to be authenticated. Every IP datagram to be sent is assigned a MD that is generated out of the datagram plus an appropriate (either secret or public) key2. At the receiver a new MD is calculated out of the datagram plus the appropriate key as known by the receiver. If the two calculated MDs are equal, it means the datagram was unaltered during transit and that only the senders that know the key could have sent it. The IP AH Format is depicted in Fig. 2 [2], [4]. The Next Header is an 8-bit field that identifies the type of the next payload after the Authentication Header. The Payload Length is an 8-bit field that specifies the length of AH in 32-bit words. The Reserved field is a 16-bit field reserved for future use. The Security Parameter Index (SPI) is an arbitrary 32-bit value that uniquely identifies the Security Association (SA) for this datagram. Sequence Number is an unsigned 32-bit field that contains a counter value that is defined for replay-protection purposes. Authentication Data is a variable-length field that contains the Integrity Check Value (ICV) for the packet.

The location of AH in IP datagrams depends on the version of IP and whether or not tunneled mode is used.

For the sake of secure mobile IP understanding, Fig. 3 illustrates how an authenticated, tunneled IPv4 packet looks like. Note that AH does not support any form of encryption and, hence, it cannot protect the confidentiality of the data sent over the Internet.

Next Header	Payload Length	RESERVED
Security Parameters Index (SPI)		
Sequence Number Field		
Authentication Data (variable)		

Fig. 2 IP Authentication Header Format

(new) IP Header	Authent. Header	(orig.) IP Header	TCP/UDP Header	User Data
<----------Authenticated---------->				

Fig. 3 Authenticated Tunneled IPv4 Packet

To this end ESP must be used. In addition to confidentiality, ESP also provides all the services provided by AH. In fact, ESP may be used in conjunction with AH.

Like the AH protocol, ESP is also designed to work with different encryption and authentication algorithms, whereas the DES-CBC transform [1], [2] is required (not mandatory!) to be used in all ESP implementations. DES-CBC stands for Data Encryption Standard-Cipher Block Chaining. Like authentication algorithms, encryption algorithms also rely on the use of keys to provide confidentiality. Once an IP datagram is encrypted, only authorized users can decrypt it, no matter which algorithm and keying mode were used.

The ESP Header is depicted in Fig. 4 [1]. The SPI and Sequence Number fields provide the same functionality as described before. Payload is a variable-length field containing data described by the Next Header field. Padding is an optional field defined to ensure that the Authentication Data field (if present) is aligned on a 4-byte boundary. The Pad Length field indicates the number of pad bytes immediately preceding it. The Next Header is an 8-bit field that identifies the type of data contained in the Payload Data field, e.g., an extension header in IPv6 or an upper layer protocol identifier. The Authentication Data is an optional, variable-length field containing an Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data.

The ESP header is inserted after the IP header and before the upper layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). For the sake of secure mobile IP understanding, Fig. 5 depicts how an ESP-encrypted, tunneled IPv4 packet looks like.

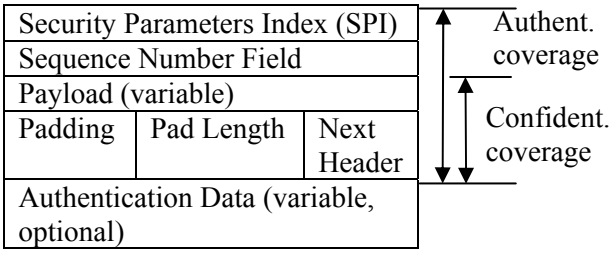

Fig. 4 IP Encapsulating Security Payload Header

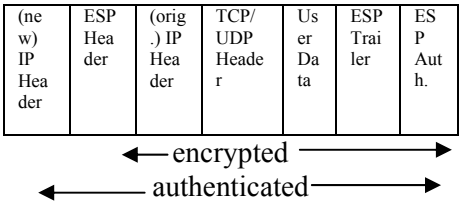

Fig. 5 Encrypted Tunneled IPv4 Packet

Fundamental to the proper functioning of the AH and ESP protocols is the concept of key sharing among communicating parties. The Internet Key Exchange (IKE) protocol has been defined such that two parties can negotiate security parameters and establish session keys thus enabling the setup of a SA. A SA is a unidirectional agreement between two communicating parties that specify a set of policies and keys to protect future communications between them. Table 1 illustrates a table of SAs identified by their SPI.

SAs can be established between end users, security gateways, end users and security gateways. Security gateways, also known as firewalls, are of fundamental importance towards secure communications over the Internet. A firewall is a device or set of devices located in the border between two administrative domains and configured in such a way that only packets with certain characteristics (e.g., IP source address, TCP ports) are allowed to enter the private domain. Different kinds of firewalls exist.

The most sophisticated and important for mobile IP is the so-called secure tunneler (see Fig. 6), a firewall which is implemented using the AH and ESP protocols. In such an architecture packets coming from the public network are processed as follow:

-If the packet is tunneled to the firewall and has valid authentication and/or encryption then it is detunneled and routed “transparently” to the destination node within the private network;

-Otherwise, the packet is submitted to the application-layer relay, a host configured to perform application-based packet filtering.

Security Parameter Index	Authent. algorithm	Authent. key
01234567	e.g., Keyed MD$	(a secret key)
89ABCDEF		

Security Parameter Index	Replay protection	Encryption algorithm	Encryption key
01234567	timestamp		
89ABCDEF		e.g., RSA	(public/ private key)

Table 1 – Security Associations

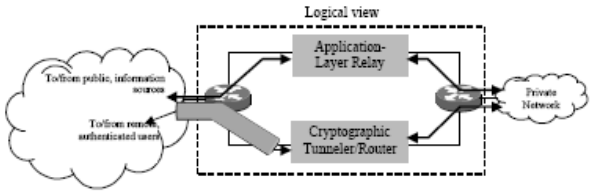

Fig. 6 Secure Tunneler

3 Mobile IP in Campus Intranets

This section discusses the application and security aspects of Mobile IP in campus intranets. Throughout this section we will use the network shown in Fig. 7 below. It is a network with no connections to the Internet, no firewalls, and has secured physical access. Furthermore, mobile node software is installed on all mobile nodes in the network, and foreign and home agent software is installed on the routers. Home addresses and home links are assigned, and shared secret encryption keys are installed. In any networked environment precautions should be taken to prevent what are called ‘insider attacks’.

Fig. 7 Network model for Mobile IP in Campus Intranets

These are attacks come from supposedly trustworthy own employees of the company, and involve unauthorized access to sensitive information for malicious purposes. Since this is not specific to mobile IP as such, we will not further discuss them here. For this network we will examine denial of service attacks (Section 3.1), passive eavesdropping (Section 3.2), session stealing (Section 3.3) and other active attacks (Section 3.4). Then we will briefly conclude on Mobile IP in Campus Intranets security aspects (Section 3.5).

3.1 Denial of Service

A popular phrased definition of a denial of service attack is 'A bad guy preventing a good guy from getting useful work done'. For computer networks in general, a denial of service attack can have two forms: a bad guy floods a host with packets (thus preventing that host from processing useful packets) or the bad guy somehow interferes with the flow of useful packets to a node. In the case of a mobile IP network a denial of service attack occurs when a bad guy manages to do a bogus registration of a new care-of address for a particular mobile node. Such a bogus registration gives rise to two problems:

· The good guy's mobile node is no longer connected;

· The bad guy gets to see all traffic directed to the original mobile node.

Denial of service by means of a bogus registration is illustrated in the Fig. 8.

The Mobile IP specification prevents bad guys from being able to do bogus registrations by requiring strong authentication on all registration messages that are exchanged during the registration process. Under the assumption that the shared secret key is not exposed, this renders this type of attack impossible. A related form of denial of service is the so-called *replay attack*.

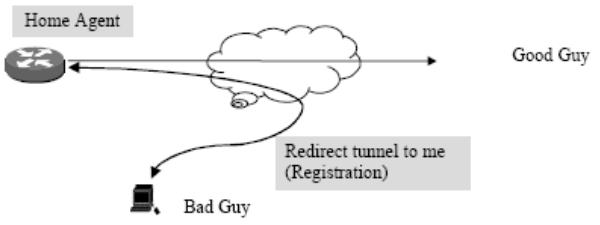

Fig. 8 – Denial of Service attack to a Mobile IP network

A replay attack occurs when the attacker records the (encrypted) registration message that a mobile node sends to the foreign agent upon visiting a network and replays that message later. Without any countermeasures this would be a feasible way of doing a denial of service attack by means of a bogus registration. Mobile IP has two ways of protection against replay attacks; the ID field of the messages is filled with either a timestamp or a nonce value. When timestamps are used the receiver of a message can determine its timeliness and thus detect and discard a replayed message. When nonces are used both parties involved agree upon what special value to use for each next message; even if the attacker knew what that next value should be, it is still impossible to insert it into an authenticated message, thereby rendering a replay attack impossible.

3.2 Passive Eavesdropping

Passive eavesdropping is a passive form of information theft. A passive eavesdropping attack occurs when a bad guy manages to listen in on traffic exchanged between a mobile node and its home agent. For this to happen an attacker needs access to the traffic; this can occur in the following ways. An attacker could get physical access to a network socket and connect a host to the network. In case of a shared Ethernet, all traffic on the segment is exposed to the eavesdropper. It is also possible that the attacker is close enough to a wireless network to be able to receive packets that are transmitted via radio signals. Reception of such radio signals is very hard to prevent. To prevent passive eavesdropping with mobile IP it is required to encrypt the transmitted information while it is in transit. An example where this is of great importance is in wireless network environments. Encrypting traffic while it is in transit can be done in various ways, as we will discuss next. As a minimum, traffic should be encrypted on the foreign link. If the traffic is encrypted on the foreign link (and under the assumption that the attacker doesn't know the cryptographic keys used for that) eavesdropping can no longer occur there. If however encryption is used only on the foreign link, the traffic is still exposed to eavesdropping on the remainder of the end to end connection. The best solution therefore is to use end to end encryption of all traffic. This renders eavesdropping attacks impossible on the complete connection. In the special case where the mobile node and the foreign agent are co-located (and therefore the foreign agent can be thrusted), encryption could be applied from the mobile node all the way to the home agent. In that case the mobile node traffic is just as secure against eavesdropping as if the mobile node was at its home location, while at the same time requiring no

changes to any of the legacy applications or system the mobile node communicates with.

3.3 Session Stealing

Session stealing is an active form of information theft. It involves a bad guy to perform the following steps:

· The bad guy waits for a mobile node to register with its home agent;
· The bad guy eavesdrops to see when something interesting comes along;
· Then the bad guy floods the mobile node with (bogus) packets, thus putting it out of action;
· The bad guy steals the session by originating packets that seem to have come from the mobile node, and at the same time intercepting packets destined for the mobile node.

Such a session stealing attack could occur either at the foreign link or at some other point between the mobile node and the home agent.

The protection against session stealing attacks is again cryptography. By encrypting the traffic on as much of the end to end connection as possible (preferably everywhere on the connection), even if a session could be stolen the attacker can not get to the actual data.

3.4 Other Active Attacks

Active attacks can be performed that do not require any existing mobile IP session to be going on. This type of attack involves getting access to the network and once that has succeeded to try and actively break into hosts on the network. Once the attacker has gained 'physical' access to the network (either via an unattended network socket or via an air interface) the procedure for this type of attack is as follows.

· The attacker figures out a network prefix to use. This can be done by listening for mobile IP agent advertisements, by examining IP addresses in packets flowing around on the network segment, or even by just doing a DHCP configuration request.
· Next the bad guy guesses an available host number to use. This can be done by listening for a while and just picking one that does not appear to be used, by doing ARP request for the resulting IP address and see if they go unanswered, or by again a DHCP request.
· Once the previous steps succeeded the attacker can start gaining access to IP hosts. For a unix system the attacker could start guessing username password combinations that work. History tells that this guessing game can in fact be successful. The relevance for mobile IP is that mobile IP is likely to be used in publicly accessible places. To prevent active attacks like just described, the following two measures need to be taken. First all publicly accessible sockets should connect to a foreign agent that enforces the 'R' bit. This means that all visiting mobile nodes are strictly required to register with the foreign agent. The foreign agent will not route any packets on behalf of nodes that have not registered with the agent. Second link layer encryption must be mandatory for all mobile nodes that wish to connect to the foreign agent.

4 Mobile IP Worldwide

In the previous section Mobile IP Deployment for an Intranet, security implications of this deployment as well as the protections against these threats have been described. In this section security threats of the intranet being extended with attack to the mobile node outside of the intranet, a protection for this mobile node as well as how this mobile node can securely access to the intranet are presented. The scenario for mobile IP worldwide however is first introduced.

4.1 Internet-wide Mobility Deployment

Mobile IP can allow a user to move anywhere through the entire Internet without exposing his Intranet to additional security threats over the attacks that face any network connected to the Internet. Fig. 9 represents an Internet-wide mobile IP deployment scenario. In the figure, we visualize the part of the Intranet with confidential data connected to the global Internet through a firewall to ensure connectivity of authorized mobile nodes. The figure also shows a public area of this Intranet that provides access for mobile nodes.

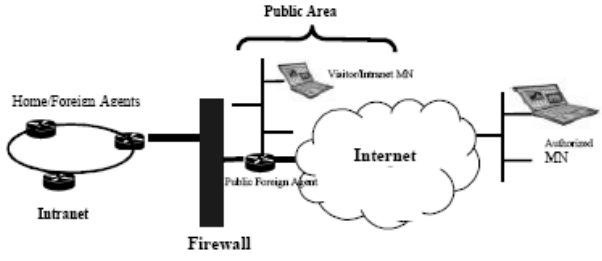

Fig. 9 - Mobile IP deployment Scenario

The mobility on Internet scenario is characterized by a topological placement of home agents and foreign agents with respect to the firewall and the mobile nodes. Although the home agents are protected by

the firewall, all foreign agents can not be under the firewall. The public foreign agent that is non-protected has to provide service to the public area's mobile nodes. Therefore this agent can support passive or active eavesdroppings. This scenario is used in the rest of this section to show how a mobile node can reach his home agent securely.

4.2 Mobile Node Protection

Although the deployment adds no security risks over and above those faced by any network that connects to the Internet, the vulnerability of the intranet with internet access introduce security threats over the network's mobile nodes that are "on the Internet" with no firewall to protect them against attacks. The protection against these threats can be a method based upon Virtual Private Networks (VPNs) technology. Fig. 10 shows VPNs for protection of Intranets. A VPN consists of two or more physical private networks that are separated by a public network and behaves as a single private network. The VPNs are built from authenticated and encrypted tunnels between secure tunneling firewalls at the border of each physical network. The firewall protects its network by admitting only those packets that have been authenticated and encrypted by one of the other firewalls.

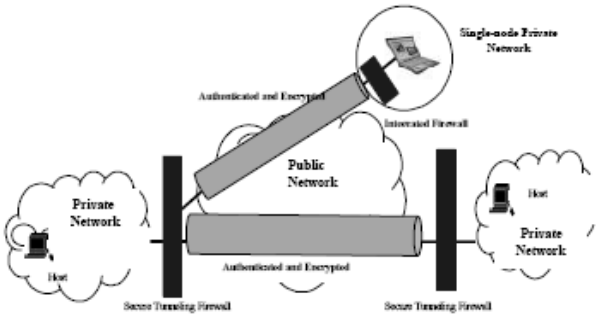

Fig. 10 - Virtual Private Network ensuring secure firewall traversal

The application of VPNs technology for a mobile node protection is also shown in this figure. In the figure the mobile node is presented as a single-node private network protected by the integrated firewall. This solution protects a mobile node through a secure tunneler. Therefore the secure tunneler is a firewall of the application-layer relay type (see fig. 6) that provides a cryptographically-protected path for authorized users to access a private network across a public network. The solution must provide a way by which the mobile node is able to communicate with all hosts and routers within the rest of the VPN (any of the physical, private networks) without compromising the security of those networks. Simple Key-Management protocol (SKIP) [9] is an implementation of the method to traverse the firewall securely. How this protocol protects the mobile node is shortly introduced in the following section.

5 Conclusion

We addressed the mobile IP security issues in campus Intranet and in the Internet. We firstly examined the ESP, the AH and the IKE protocols defined in the IETF's IPSec architecture. Based on these protocols, protection against denial of service, passive eavesdropping, session stealing and other active attacks in campus intranets were discussed. These discussions were further extended to the Internet-wide context, where the use of the secure tunneler as a main protection mechanism was examined. The recurring pattern in the counter measures against all of these attacks is that security mechanisms and services concern authentication and encryption techniques to prevent security attacks. Security mechanisms, services and protocols to provide communications throughout the Internet with confidentiality, authentication and integrity are under elaboration within the IETF. The works cover both IPv4 and IPv6 and ranges from the link layer up to the application layer.

References

[1] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 2406, December 2005.
[2] S. Kent and R. Atkinson. IP Authentication Header. RFC 4303, December 2005.
[3] Eastlake, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, December 2005.
[4] Kent, S., "IP Authentication Header", RFC 4302, December 2005.
[5] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.
[6] Krawczyk, H., "The Order of Encryption and Authentication for Protecting Communications (Or: How Secure Is SSL?)", CRYPTO' 2001.
[7] Kaufman, C., Ed., "The Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.
[8] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.