Mobile IP – Security Issues and Solutions

Sameer Chandragiri
Dept of Computer Science
University of Texas at Arlington
CSE 6345 Term Paper
samchan@rediffmail.com

ABSTRACT

In the last few years, the area of mobile computing has grown tremendously. Devices like PDAs, handhelds and digital cellular phones that started off as gadgets of luxury have become a necessity in today's "always-stay-connected" lifestyle. To facilitate mobility of such devices without disconnection from the network, Mobile IP came into existence. This allows the mobile node to use two IP addresses: a fixed home address and a care-of address that changes at each new point of attachment. But with the advantages of Mobile IP also came the disadvantages, the biggest of them being that of security. In this paper, we discuss a few of the common security threats that mobile IP networks are exposed to as well as some proposed solutions to deal with such threats.

1. INTRODUCTION

While offering great flexibility and potential, mobility exposes mobile nodes and consequently entire networks to various security threats. Combat against such threats requires appropriate services and protocols. Some of the problems are solvable today. However others might require more research to actually lead to practical and feasible solutions.

The remaining sections of the paper discuss the various security issues that pose a threat to secure and meaningful Mobile IP operations, especially focusing on Mobile IP in campus Intranets. A few proposed solutions are also discussed.

2. DENIAL OF SERVICE

A simple 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 Figure 1.

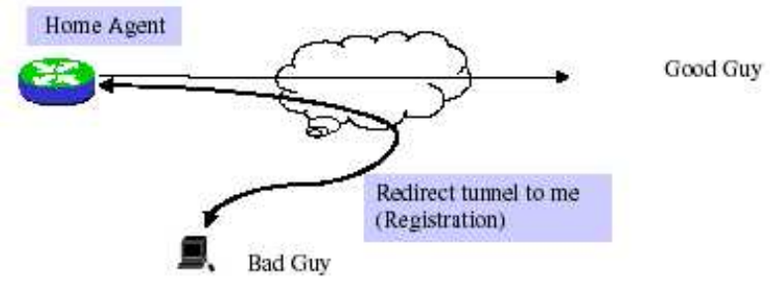

Figure 1 – Denial of Service attack to a Mobile IP network

A related form of denial of service is the so-called *replay attack.* This kind of 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. This is as good as registering a bogus care-of address for the mobile node.

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. In this case, unless the shared key is exposed, this type of attack is rendered impossible.

To prevent a replay attack, the Identification field is generated is a such a way as to allow the home agent to determine what the next value should be. The identification field can be filled with either a timestamp or a nonce value. In this way, the bad guy is thwarted because the

Identification field in his stored Registration Request will be recognized as being out of date by the home agent.

3. 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. This can be done in various ways. As a minimum, traffic should be encrypted on the foreign link. Assuming that the attacker does not know the cryptographic keys used for the traffic, eavesdropping can no longer occur on the foreign link. However, the traffic is still exposed to eavesdropping on the remainder of the end to end connection.

Therefore the best solution would be to use end to end encryption of all traffic. This renders eavesdropping attacks impossible on the complete connection.

4. SESSION STEALING

Session stealing is an active form of information theft. It involves the following steps:

- The Bad Guy waits for a mobile node to register with its home agent
- The Bad Guy eavesdrops to see if the mobile node has any interesting conversation taking place (remote login session to another host, connection to the electronic mailbox)
- The Bad Guy floods the mobile node with nuisance (bogus) packets

- The Bad Guy steals the session by sending the packets that appear to have come from the mobile node and by intercepting packets destined to the mobile node

The protection against session stealing attacks is again similar to that for passive eavesdropping, i.e. cryptography. Minimally, link-layer encryption between the mobile node and the foreign agent should be provided to avoid session stealing on the foreign link.

5. OTHER ACTIVE ATTACKS

Active attacks involve getting access to the network and once that has succeeded, to try and actively break into hosts on the network. These type of attacks do not require any existing mobile IP session to be going on. Once the attacker has gained physical access to the network the procedure for this type of attack is as follows:

- The attacker figures out the network-prefix that has been assigned to the link on which the network jacks are connected.
- He/she guesses a host number to use which combined with the network-prefix gives him/her an IP address to use on the current link.
- The attacker finally tries to gain access to IP hosts by probably trying various combinations of user-name/password pairs. This is not an impossible task as there are a lot many software applications today that continuously generate different random combinations of username/password pairs till one combination works.

To prevent active attacks like just described, the following two measures need to be taken. Firstly, all publicly accessible sockets should connect to a foreign agent that enforces the ‘R’ bit i.e. all visiting mobile nodes are strictly required to register with the foreign agent. Secondly, link layer encryption must be mandatory for all mobile nodes that wish to connect to the foreign agent.

6. CONCLUSION

Security in Mobile IP is one of the major challenges in Mobile IP today. We have discussed a few issues that are more so prevalent in campus intranets. We have also outlined a few solutions for each of the discussed issues. A lot of research still needs to be done in this area. Security in mobile IP is still not free from loopholes.

7. REFERENCES

1. Charles E. Perkins, Mobile Networking through Mobile IP
2. Gloria Tuquerres, Marcos Rogério Salvador and Ron Sprenkels, Mobile IP: Security & Application, 1999