Analysis of Authentication Protocols in Mobile IP

Lalit Kumar
Assistant Professor
Department of Computer Science & Engineering
GZS-PTU Campus, Bathinda (Punjab)
lalitbti@gmail.com

Abstract- *Mobile Internet Protocol (IP) is a new recommended Internet protocol designed to support the mobility of a user (host). Host mobility is becoming important because of the recent blossoming of laptop computers and the high desire to have continuous network connectivity anywhere the host happens to be. The development of Mobile IP makes this possible. This paper describes and summarizes the characteristics of the current Internet draft for Mobile IP. In addition to the current internet draft, this paper also discusses authentication mechanism in Mobile IP proposals so that the reader may understand the different design issues associated with the different authentication protocols.*

Keywords- *Internet Protocol, Mobile IP, Internet, authentication protocols.*

INTRODUCTION

Background -- The Problem with Old IPs is that Current internet protocol versions do not support host mobility. These were designed such that moving hosts were not considered: a node's point of attachment to the network remains unchanged at all times, and an IP address identifies a particular network. To support a mobile host with current methods, reconfiguration is necessary any time a mobile host moves. This is an unacceptable solution as it is time consuming and error prone. Thus, the rise of Mobile IP.

Mobile IP is an internet protocol designed to support host mobility. Its goal is to provide the ability of a host to stay connected to the internet regardless of their location. Mobile IP is able to track a mobile host without needing to change the mobile host's long-term IP address.

Features:

- No geographical limitations
- No physical connection required
- Modifications to other routers and hosts is not required
- No modifications to the current IP address and IP address format
- Supports security

Entities and Services

Mobile IP is consisting of the following entities:

Mobile Node (MN)

A host or router that may change its point of attachment from one network or sub network to another through the internet. This entity is pre-assigned a fixed home address on a home network, which other correspondent hosts will use to address their packets to, regardless of its current location.

Home Agent (HA)

A router that maintains a list of registered mobile nodes in a visitor list. It is used to forward mobile node-addressed packets to the appropriate local network when the mobile nodes are away from home. After checking with the current mobility bindings for a particular mobile node, it encapsulates datagram's and sends it to the mobile host's current temporary address when the mobile node.

Foreign Agent (FA)
A router that assists a locally reachable mobile node that is away from its home network. It delivers information between the mobile node and the home agent.

Care-of-address (COA)
An address which identifies the mobile node's current location. It can be viewed as the end of a tunnel directed towards a mobile node. It can be either assigned dynamically or associated with its foreign agent.

Correspondent Node (CN)
This node sends the packets which are addressed to the mobile node.

Tunnel
The path which is taken by encapsulated (see below) packets. It is the path which leads packets from the home agent to the foreign agent.[1]

PROBLEMS OF BASE MOBILE IP PROTOCOL

Mobile IP still has many items that need to be worked on and enhanced such as the security issue and the routing issue. The IETF has been working on the problems which had been found on the base Mobile IP protocol.
Triangle routing: As noted above, datagram's going to the mobile node have to travel through the home agent when the mobile node is away from home, but datagram's from the mobile node to other stationary Internet nodes can be routed directly to their destinations. This additional routing, called triangle routing and shown in Figure 1, is generally far from optimal, especially in cases when the correspondent node is very close to the mobile node. Route Optimization is the protocol suggested to eliminate the triangle routing problem and is described here.

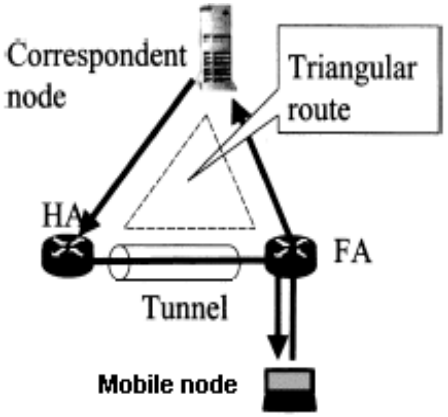

Figure 1: Triangle routing

Security issues: The most pressing outstanding problem facing Mobile IP is that of security. A great deal of attention is being focused on making Mobile IP coexist with the security features coming into use within the Internet. Firewalls in particular cause difficulty for Mobile IP because they block all classes of incoming packets that do not meet specified criteria. Although this permits management of internal Internet nodes without great attention to security, it presents difficulties for mobile nodes wishing to communicate with other nodes within their home enterprise networks. Such communications, originating from the mobile node, carry the mobile node's home address and would thus be blocked by the firewall.

A Comparative authentication mechanism on Mobile IP

- EAP-TLS(Extensible Authentication Protocol- Transport Layer Security)
- Kerberos v5
- SSH(Secure Shell)

EAP-TLS

- EAP is a widespread authentication protocol especially with Transport Layer

Security (TLS), which is called by EAP-TLS. For the purpose of the mutual authentication, most wireless technologies such as IEEE 802.11 and IEEE 802.16 adopt EAP-TLS as the authentication protocol.

Kerberos

- Kerberos is an authentication service especially for open distributed environments .It is an Key- Distributed Protocol. This can achieve that the user types her ID and password once, and acquires the authority to obtain the various services from the distributed service servers

SSH

- SSH, the Secure Shell, is a popular, powerful, software -based approach to network security - SSH has client/server architecture. An SSH *server* program, typically installed and run by a system administrator, accepts or rejects incoming connections to its host computer. Users then run SSH *client* programs, such as "Please log me in," "Please send me a file," or "Please execute this command." typically on other computers, to make requests of the SSH server based approach to network security. [3]

PERFORMANCE COMPARISON

In this section, we evaluate the authentication costs for the proposed authentication mechanism, Kerberos, and EAP-TLS.

Mobile IPv6 (MIPv6) is the most outstanding protocol in a general tendency of the mobility management area. MIPv6 is the network-based localized mobility management protocol developed by the IETF. MIPv6 introduces two entities which are Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA). MAG is an access router that is charged with sending and receiving the mobility signaling by the deputy of the MN. LMA performs the management of the mobility service—the binding services and data tunneling.

Applying EAP-TLS to PMIPv6

EAP is a widespread authentication protocol especially with Transport Layer Security (TLS), which is called by EAP-TLS. For the purpose of the mutual authentication, most wireless technologies such as IEEE 802.11 and IEEE 802.16 adopt EAP-TLS as the authentication protocol. EAP-TLS can be applied also to the MIPv6 environment. The message sequence when EAP-TLS is applied to the MIPv6 environment. EAP method starts the negotiation with the EAP request message from the Access Point (AP). With the EAP negotiation, the MN and the AS determine to use EAPTLS as the authentication protocol. After the negotiation, the MN and the AS exchange their certificate to achieve the mutual authentication and the key exchange. More precise meaning of each message can be found in. With EAP-TLS, the method for the validation and revocation of the certificate must be provided. Moreover, the MN has to be authenticated with same procedure whenever the MN moves to the territory of other MAGs, which means that the MN and the AS must validate each certification every time.

Applying Kerberos to MIPv6

Kerberos is an authentication service especially for open distributed environments. This can achieve that the user types her ID and password once, and acquires the authority to obtain the various services from the distributed service servers. If the MAGs are thought to be the service servers, we can apply Kerberos simply to MIP environments. Here, we assume that the ticket-granting server and the AS are in the

same entity. More precise meaning of each message can be found in.
However, the MAGs are treated as independent service servers if there is no reorganization of the mechanism. Thus, the MN must be granted the authority to be provided the network service from the ticket-granting server whenever the MN changes its attachment.

Comparing SSH and Kerberos
While they solve many of the same problems, Kerberos and SSH are very different systems. SSH is a lightweight, easily deployed package, designed to work on existing systems with minimal changes. Kerberos, in contrast, requires you to establish a significant infrastructure before use.
Infrastructure
Let's consider an example: allowing users to create secure sessions between two machines. With SSH, you simply install the SSH client on the first machine and the server on the second, start the server, and you're ready to go. Kerberos, however, requires the following administrative tasks:

- Establish at least one Kerberos Key Distribution Center (KDC) host. The KDCs are central to the Kerberos system and must be heavily secured; typically they run nothing but the KDC, don't allow remote login access, and are kept in a physically secure location. Kerberos can't operate without a KDC, so it is wise to establish backup or "slave" KDCs also, which then must be synchronized periodically with the master. A KDC host might also run a remote administration server, a credentials-conversion server for Kerberos-4 compatibility in a Kerberos-5 installation, and other server programs depending on your needs. Although, if remote login access to a KDC is desired, SSH is a good way to do it!

Security of authenticators
The extra complexity of Kerberos provides properties and capabilities that SSH doesn't. One major win of Kerberos is its transmission and storage of authenticators (i.e., passwords, secret keys, etc.). To demonstrate this advantage, let's compare Kerberos's *ticket* system with SSH's password and public-key authentication.

SSH password authentication requires your password each time you log in, and it is sent across the network each time. The password isn't vulnerable during transmission, of course, since SSH encrypts the network connection. However, it does arrive at the other side and exist in plaintext inside the SSH server long enough for authentication to occur, and if the remote host has been compromised, an adversary has an opportunity to obtain your password.

Performance
Kerberos authentication is generally faster than SSH public-key authentication. This is because Kerberos usually employs DES or 3DES, whereas SSH uses public-key cryptography, which is much slower in software than any symmetric cipher. This difference may be significant if your application needs to make many short-lived secure network connections and isn't running on the fastest hardware.

To sum up: Kerberos is a system of broader scope than SSH, providing authentication, encryption, key distribution, account management, and authorization services. It requires substantial expertise and infrastructure to deploy and requires significant changes to an existing environment for use. SSH addresses fewer needs, but has features that Kerberos installations typically don't, such as port forwarding. SSH is much more easily and quickly deployed and is more useful for

securing existing applications with minimal impact.

Using Kerberos with SSH

Kerberos is an authentication and authorization (AA) system. SSH is a remote-login tool that performs AA as part of its operation, and one AA system it can use is (you guessed it) Kerberos. If your site already uses Kerberos, its combination with SSH is compelling, since you can apply your existing infrastructure of principals and access controls to SSH.[5]

Even if you're not already using Kerberos, you might want to roll it out together with SSH as an integrated solution because of the advantages Kerberos provides. By itself, the most flexible SSH authentication method is public-key with an agent. Passwords are annoying and limited because of the need to type them repeatedly, and the trusted-host method isn't appropriate or secure enough for many situations. Unfortunately, the public-key method incurs substantial administrative overhead: users must generate, distribute, and maintain their keys, as well as manage their various SSH authorization files. For a large site with many nontechnical users, this can be a big problem, perhaps a prohibitive one. Kerberos provides the key-management a feature SSH is missing. SSH with Kerberos behaves much like public-key authentication: it provides cryptographic authentication that doesn't give away the user's password, and the ticket cache gives the same advantages as the key agent, allowing for single sign-on. But there are no keys to generate, authorization files to set up, or configuration files to edit; Kerberos takes care of all this automatically.

CONCLUSIONS

The Mobile IPv6 has been established, and now the biggest issue is what about the security. In this paper, we review, analyze and discuss the authentication protocols and the security issues about Mobile IPv6. We have introduced the three authentication mechanism for MIPv6. These mechanisms discuss the inefficiency caused by the authentication whenever an MN changes its attachment point.

REFERENCES

[1]. Fayza A. Nada "On using Mobile IP Protocols" Faculty of Computers and Information, Suez Canal University, Ismailia, Egypt Journal of Computer Science 2 (2): 211-217, 2006 ISSN 1549-3636 (c) 2006 Science Publications

[2]. Charles Perkins, The Internet Mobile Host Protocol (IMHP), Internet Draft, 2002. This draft specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet

[3] Huiping Sun; Junde Song; Zhong Chen; "Survey of Authentication in Mobile IPv6 Network" Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE, Digital Object Identifier: 10.1109/CCNC.2010.5421695 Publication Year: 2010, Page(s): 1 - 4

[4]. Joong-Hee Lee; Jong-Hyouk Lee; Tai-Myoung Chung; "Ticket-Based Authentication Mechanism for Proxy Mobile IPv6 Environment" Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on Digital Object Identifier:10.1109/ICSNC.2008.25 Publication Year: 2008, Page(s): 304 – 309

[5]. Overview of SSH Features (SSH, The Secure Shell: The Definitive Guide) by Daniel J. Barrett and Richard E. Silverman ISBN: 0-596-00011-1 First edition, published February 2001, ch01