Security policy for deducting unauthorized IP based mobile host inside the network

V.K. SANJEEVI*, VELUCHANDHAR**, S.SAKTHIVEL ***, M. SUPRIYA ***
* General Manager, BSNL ,**Department of Computer Science, St.Joseph’s College (Autonomous) Tiruchirappalli ,***Wipro Info Tech, Bangalore, India

Abstract: - The technology evaluation of mobile management system has integrated with significant improvement in mobile computing. The requirements for mobile security are more important when we are accessing the sensitive data from the database. Concurrency control ensures that individual users meet consistent states of the mobile databases with security. But in the IP based mobile network the relay of data is not continuous and also the connection may lose at any time. The IP alone is not suitable for identifying the mobile host inside the network. In this paper, it is proposed a model to enhance the performance of mobile security for IP based mobile host.

Key-Words: - Mobile security, IP based mobile hosts, Mobile hacking, Security policy, Mobile IP security problems

1 Introduction
Mobile Computing is becoming increasingly important due to the rise in the number of portable computers and the desire to have continuous network connectivity to the Internet irrespective of the physical location of the node. The Internet infrastructure is built on top of a collection of protocols, called the TCP/IP protocol suite. IP requires the location of any host connected to the Internet to be uniquely identified by an assigned IP address.

The mobile hosts cannot currently interoperate easily or conveniently with internetworking protocols such as IP due to the operation of existing internetwork addresses and routing algorithms. For example, in IP, host addresses are composed of a network number, identifying the network to which the host is attached, and a host number, identifying the particular host within that network. IP expects to be able to route a datagram to a host based on the network number contained in the host’s IP address. If a host changes its point of connection to the Internet and moves to a new network, IP datagrams destined for it will no longer reach it correctly.

This raises one of the most important issues in mobility, because when a host moves to another physical location, it has to change its IP address. However, the higher level protocols require IP address of a host to be fixed for identifying connections. The Mobile Internet Protocol (Mobile IP) is an extension to the Internet Protocol proposed by the Internet Engineering Task Force (IETF) that addresses this issue. It enables mobile computers to stay connected to the Internet regardless of their location and without changing their IP address. More precisely, Mobile IP is a standard protocol that builds on the Internet Protocol by making mobility transparent to applications and higher level protocols like TCP.

The paper is organized as follows: The review of literature on Mobile Security and related issues on Mobile IP are presented in the Section-2. Section-3 presents the proposed security policy for Mobile IPI. Section-4 concludes paper.

2 Review of literature
The operations of the data transmission can be performed in the form of packets. The packets are sent to the mobile host using the IP address. This can be performed under supervision of the network agents. The Wired Equivalent Privacy protocol is used in 802.11 networks to protect link-level data during wireless transmission. It is described in detail in the 802.11 standard. The claimed security of the WEP protocol “relies on the difficulty of discovering the secret key through a brute-force attack” [1].

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 [2]. The AH protocol is designed to work with many different authentication algorithms, whereas the most used is the mandatory Message Digest (MD) 5 [3]. Mobile IP is based on the idea of providing mobility support on the top of existing IP infrastructure, Without
Host security is a reasonably well researched issue, and many viable mechanisms have been developed to address it. Examples of such mechanisms include sandbox security (used in Java to provide access control) [5], safe-typed languages [6] and proof-carrying code [7].

Code security is however more problematic, since this aspect has only come into prominence recently as a security problem unique to mobile code. Some of the more well known mechanisms used to overcome this problem include code obfuscation [8], encrypted functions [9], execution tracing [10] and tamper resistant hardware [11], [12]. It is likely this area will be crucial in determining the future viability of mobile agent application in e-commerce scenarios.

An overview of the current techniques available to address both host axtd code security is provided in [13] and [14]; the reader is referred to them for a summary of these techniques as well as a discussion of their corresponding advantages and drawbacks.

3 Proposed model

While Internet technologies largely succeed in overcoming the barriers of time and distance, existing Internet technologies have yet to fully accommodate the increasing mobility of people with their computers. A promising technology used to eliminate this current barrier is Mobile IP.

At the same time, the Internet (TCP/IP protocol stack) was not designed for wireless (less mobile) networks; instead it was designed for fixed-wired networks. Therefore, despite a core IP protocol's flexibility, wireless and mobile networks require certain changes to the standard TCP/IP.

The emerging 3G mobile networks are set to make a huge difference to the international business community. 3G networks will provide sufficient bandwidth to run most of the business computer applications providing a reasonable user experience. However, 3G networks are not based on only one standard, but a set of radio technology standards such as cdma2000, EDGE and WCDMA. It is easy to foresee that the user from time to time also would like to connect to fixed broadband networks, wireless LANs and, mixtures of new technologies such as Bluetooth connected to e.g. cable TV and DSL access points.

Criminals leverage new attack vectors as soon as old vectors dry up. Over time, the good guys shut their doors and install better locks. In this century developers strengthened their defenses and attackers focused their attention elsewhere. The defenses we’ll see over the next few years are not total solutions; however, they are significant deterrents that will again shift the focus. New technologies appear at an explosive pace, and many of the attack vectors—and their defenses—haven’t yet been explored. We are at the beginning of a new era in the cat-and-mouse game. Cybercrime is not limited to laptop and desktop computers. It includes devices such as cell phones and MP3 players. Today, the majority of cybercriminals target PC users, but we can expect more attackers to branch out to other areas of technology during the coming years as those technologies become more widely adopted.

3.1 IP and Mobile Host

The IP address is playing the major role to identify the mobile host. IP routing was originally defined, mobility of hosts was not considered to be an issue. Routing methods were built for static networks, where the hosts were unlikely to move from one subnet to another. Routing takes advantage of a “network number” contained in every IP address. Thus, the IP address encodes the computer’s physical location and - by default - the location is fixed. The basic Mobile IP protocol has four distinct stages. These are:

Agent Discovery: The mobile node receiving the Agent Advertisement message observes whether the message is from its own home agent and determines whether it is on the home network or a foreign network.

Registration: If the mobile node is on a new network, it registers with the foreign agent by sending a Registration Request message which includes the permanent IP address of the mobile host and the IP address of its home agent.

In Service: When the mobile node wants to send a message to a correspondent node, it forwards the packet to the foreign agent, which in turn relays the packet to the correspondent node using normal IP routing.

Deregistration: If a mobile node wants to drop its care-of address, it has to deregister with its home agent. It achieves this by sending a Registration Request with the lifetime set to zero. There is no need for deregistering with the foreign agent as registration automatically expires when lifetime becomes zero. However if the mobile node visits a new network, the old foreign network does not know the new care-of address of the mobile node. Thus datagrams already forwarded by the
home agent to the old foreign agent of the mobile node are lost.

3.2 The Security Policy for IP based Mobile Devices

The IP based mobile devices are identified using the IP inside the network. The handoff procedure rises, if the mobile host is moving from one network to another. The adjacent networks are waiting for the mobile host with the same IP.

The IP address and other security related details are transmitted to neighborhood networks. There is a possible of unauthenticated mobile host with same IP address can enter into the network, when the authenticated mobile host is inside the non coverage area. This is shown in the Figure 1. We need some mechanism to identify the unauthorized mobile host inside the network. We have to introduce new protocol for IP based mobile network for overcome the hacking methods.

3.3 Security Policy for IP based mobile host

The proposed policy should having both IP and a unique number for identifying the mobile host. The unique number should be dynamically generated by home agent. The mobile host is accepted by the remote host only when the security number and the IP address is correct. The figure 2 describes the various stages in the security model.
• The handoff procedure is raised when the host is unavailable.
• The mobile host sends the request for resume connection.
• The connection is established when the IP and security number is correct otherwise the connection is dropped.

3.4 Algorithm for security number based security policy

\[
\text{function generateSecurityNumber(IPaddress, DevicePhysicalNumber)} \\
\quad \_\text{randomNumber=}\text{Random()} \\
\quad \_\text{encryptIP=}\text{encryptIp(IPaddress, randomNumber)} \\
\quad \_\text{encryptDPN=}\text{encryptDPN(DevicePhysicalNumber, randomNumber)} \\
\quad \text{return hash(\_encryptIP, \_encryptDPN)} \\
\text{end function}
\]

\[
\text{function SecurityPolicy()} \\
\quad \_\text{SecurityNumber=}\text{requestNewConnection(IPaddress, DevicePhysicalNumber)} \\
\quad \text{transmitData()} \\
\quad \text{listen event hostMoving()} \\
\quad \text{listen event hostResumeRequest()} \\
\text{end function}
\]

In the proposed security model, the unauthorized mobile with same IP address is identified and can be eliminated from the network. In addition we can alert the administrator for the intrusion of the unauthorized mobile host.

3.5 The TCP/IP header for Mobile IP

In the TCP/IP protocol at the IP layer, the IP packet is made up of two parts: the IP header and the IP body, as shown in Figure 3. From a packet filtering point of view, the IP header contains four interesting pieces of information:
The IP source address - four bytes long, and typically written as something like 172.16.244.34.
The IP destination address - just like the IP source address.
The IP protocol type - identifies the IP body as a TCP packet, as opposed to a UDP packet, an Internet Control Message Protocol (ICMP) packet, or some other type of packet.
The IP options field - which is almost always empty, but which is where options like the IP source route and the IP security options would be specified if they were used for a given packet. (See the discussion in "IP options" below.)

So we need a change in the structure of TCP/IP header. We need some more space for storing the security number inside the TCP/IP header. So we can easily check the authenticated mobile host.

<table>
<thead>
<tr>
<th>16-bit</th>
<th>32-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Destination Port</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>Acknowledgement Number (ACK)</td>
</tr>
<tr>
<td>Offset Reserved</td>
<td>AP</td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent Pointer</td>
</tr>
<tr>
<td>Options and Padding</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3

5. CONCLUSION

Mobile hosts today play a reality. Several organizations are now implementing mobile based data transmissions. Security is a serious concern a while accessing data. Different security policies need to be integrated into the security system to avoid access conflict. We have proposed a new model for Secured Mobile access. This model can be applied for any real-time environment such as, corporate, financial enterprises, academic institute etc., and performing day-to-day mobile transactions cutting edge to different levels of security.

References:


