IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 9, September 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009007|

Security Issues with Mobile IP

Mantasha Asrar Khan[1], Priyanka Ajit Chavan[2]

Department of Information Technology,B.K. Birla College of Arts,Science & Commerce(Autonomous), Kalyan, Maharashtra, India

ABSTRACT: In last few years the growth in wireless technology has led to increase in mobile users tremendously. Its use and requirement have taken a use huge growth and are becoming need of people.Apart from battery and power consumption being the main issue, security is also one of the major concerns nowadays.As Mobile IP use open airwaves as a mode of transmission, it is open to many threats.
In this paper,we have discussed the major security attacks on Mobile IP. Furthermore, we have also given solutions to security problems,and we go further to discuss the counter claims in an effort to convince the reader that the advantage of Mobile IP outweighs its disadvantages

KEYWORDS: Mobile IP, Security Issues, Solutions, Attacks

I.INTRODUCTION

In the present wireless networks, when a mobile node goes from one access point to another, the connection is reestablished each time with a different IP address. Due to this, there is a delay between the user's action and a web application response to it, thus provides an interrupted service. The need for uninterrupted communication when a node moves from one network to another involves a replacement technology. Mobile IP allows users to maneuver from one network to another with the same IP address. Mobile IP allows users to vary access points without the connections being dropped. Mobile IP is created by extending the standard internet protocol proposed by the Internet Engineering Task Force(IETF). But at a similar time, there are many security threats.
In this paper, we will discuss the working of mobile IP, security issues caused by mobile IP. Then we've given some solutions to the issues and suggestions for improving the security of mobile IP.

Mobile IP:
Mobile IP is an open standard communication protocol defined by Internet Engineering Task Force (IETF) that permits mobile device users to move from one network to another without changing their IP address as a change in the IP address will interrupt ongoing communications.
We must understand few terminologies before understanding the working of mobile IP.Terminologies:

Mobile Node: It is the device carried by the user.eg- cell phone
Home Network: It's a network to which the mobile node originally belongs.
Home Agent (HA): It is a router in the home network.

Home Address: It is the permanent IP address of the mobile node.

Foreign Network: It's the present network to which the mobile node has visited.

Foreign Agent (FA): It is a router in a foreign network to which the host is currently connected.

Correspondent Node (CN): It's a device on the internet which is communicating with the host.

Care-of Address (COA): It's a temporary IP address employed by the host.

When the correspondent node sends the data to the mobile node, packets reach the home agent. But now the mobile node is not in the home network, it has moved to the foreign network. The foreign network will send care of address (temporary IP address) to the home agent. Hence a tunnel is established between the home agent and foreign agent.
Now the home agent will encapsulate data and send it to the foreign agent through the tunnel. This process is named **tunnelling**. Once the packets reach the foreign agent, it will decapsulate the packets and send it to the

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009007|

mobile node. As the mobile node has received the data packets, it will send a reply to the foreign agent. The foreign agent will directly send the reply to the correspondent node.

Route optimisation in mobile IP

Route optimization provides developments to the routing of datagrams among the mobile node and the correspondent node. Whenever the home agent receives a data packet that has to be sent to the mobile node which is in the foreign network, it will send an update to the corresponding node to update information in its binding cache. After this, the correspondent node can directly send packets to the mobile node.

Need for mobile IP

While implementing the IP addressing system it was considered that the host would be stationaryand would stick to the 'specific network' only. But when the mobile node moves to a foreign network, its IP address becomes invalid. So, how it can communicate with the correspondent node? Below two solutions have been given for this problem:

1) Changing the IP address every time the mobile node enters a foreign network. This effort was not successful as it has several downsides. Every time the computer enters a foreign network it has to be rebooted. If the mobile node moves to a foreign network in between the data transmission, the data exchange would be disrupted.
2) Here the mobile node will have two IP addresses, the first is the permanent IP address of the mobile node, and the second is the temporary address provided when the mobile node is in a foreign network.

So, the Mobile IP protocol allows a host to move to the foreign network by retaining its original IP address and still communicate with the other hosts over the internet.

II. METHODOLOGY

Security issues with Mobile IP

1)Denial-of-Service Attack (Dos):

Denial-of-Service attacks are carried to shut down a system or network. This attack intends to make the system unavailable for its valid users by crashing the system. Although no significant loss of data occurs due to this attack. But user requires a lot of time and money to tackle such attacks. It becomes very challenging to discover the attacking party. These attacks usually target government and trade organizations, banks, etc. DOS attack is usually done by flooding the system or network with traffic or making it crash. Here are some flood attacks:

Buffer overflow attacks- In this attack, the system is flooded with network traffic so that the buffer gets overloaded and shuts down.

SyN flood- In this, a request is sent to get connected to a server and never finalize the connection. It is carried on until all ports are saturated with requests resulting in huge traffic. So that the server uses all its assets to get connected to the requests and legitimate users cannot connect to it.

DOS attacks can be prevented by securing the network, practice basic network security, alertness, slowing down of a network for more than usual time, etc should be noticed.

2)Insider attack:

An insider attack is an attack that is done by the insiders (employee or person) inside an organization who has inside information regarding security, data, and system. This attack is very malicious to an organization. This attack is done for financial purposes or other gains thus damaging the reputation of the company. Insider attacks can be minimized by giving the least amount of access to the employees. The employees should be given only that much access which is required for their job. Many a time insider attacks also occur because the employee or anyone who has been given access inserts an infected pen drive, clicks on a suspicious link, or downloads a malicious file. Hence employees must be well-aware. Behavior analysis is also very important.

3)Replay attack

A replay attack is an attack in which a hacker captures the traffic and sends a malicious message to the receiver, the receiver feels that the message is from the original user. The name is given replay attack because the receiver receives two messages-one from the original sender and the other from a hacker. Replay attack can be prevented using the session key method i.e., here only a sender and receiver can use the key and it cannot be reused.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009007|

4)Theft of information attack

When a hacker intercepts the data which is being transmitted between two devices, an eavesdropping attack occurs. It is also called sniffing. The hackers can do this attack when users use unsecured network connections like free wi-fi, which gives an opportunity to the hackers to intervene in communications. It becomes very hard to search the hackers. Hackers can steal sensitive information such as banking information, passwords and various data which can lead to financial losses. Through this attack, attackers can also listen to our communication. These attacks can be prevented by using firewalls, VPNs, keeping strong passwords, and keeping antivirus updated. Public Wi-Fi should be avoided. Banking transactions and sensitive data should not be exchanged over free Wi-Fi. One should avoid untrusted links. Keep your phone to its latest updated version of OS(operating systems).

Solutions for security issues with mobile IP

1)Using VPNs:

VPN (virtual private network) is used for mobile node protection. VPN gives you online protection and security by creating a private network from a public web association. They act as a single private network. VPNs cover your IP address so your online actions are untraceable. Generally significant, VPN services set up secure and encrypted connections to give more privacy than even a secured Wi-Fi connection. Without a VPN your internet service provider can track your search history and browsing history. But with a VPN your history is concealed. Thus VPNs keep your activities private.

VPNs create a tunnel between your mobile node and correspondent node which could be anywhere in the network. VPNs encrypt the data when it is sent over a network, so no one can read your data except the person whom you have sent.

2)Firewall:

Firewalls examine approaching traffic based on pre-defined rules. They filter the traffic coming from unsafe sources to prevent attacks. Firewalls shields traffic at a computer's ports where communication takes place with outside devices. Firewalls do this task by allowing or blocking specific data packets based on the pre-defined set of rules. Approaching traffic is allowed only through trustedIP addresses or trusted sources. They guard the device against malware. We can strengthen the security of mobile IPs using different firewalls. There are various types of firewalls:

Proxy firewall-Proxy firewalls channel network traffic at the application level hence they are also known as application firewalls. In contrast to basic firewalls, the proxy firewall acts as an intermediary between two endpoints. The client sends a request to the firewall, where it is examined against a set of rules and then given permission or blocked. A proxy firewall has its IP address, so an outside network connection will never receive packets directly from the sending network. They make sure that only authorized sources approach the resources of a computer.

Network address translation (NAT)firewallsuse routers for security. keeping singular IP addresses hidden. Thus attackers can't access specific details, thus giving more protection against attacks. NAT firewalls are similar to proxy firewalls. They act as a mediator between a group of computers and outside traffic. It doesn't make visible internal IP addresses to the internet.

SMLI (stateful multi-layer inspection)firewall- The stateful multi-layer inspection (SMLI) checks all the layers of OSI model. It analyses the entire packet whereas other firewalls just examine the packet header. Thus it examines that communication occurs with safety devices.

Cloud firewall- cloud firewall examines approaching traffic based on pre-defined rules. They form a protective shield in the cloud platforms just like other firewalls form a barrier in a network. They run in the cloud. They are also known as firewall-as-a-service (FWaaS). They protect sensitive data from getting leaked. They integrate easily with cloud infrastructure. They do not need a hardware appliance. In the world of cloud computing, traditional firewalls are failing to protect digital assets. They protect data stored on clouds from cyber-attacks. The various benefits of cloud-based firewalls are easy Deployment and Scalability, automatic updates, migration security, performance management, etc.

3)Avoiding route optimization:

Route optimization has been recently introduced. Whenever the home agent receives a data packet which has to be sent to the mobile node which is in the foreign network, it will send an update to the corresponding node to update information in its binding cache. After this, the correspondent node can directly communicate with the mobile node. However, the main problem with route optimization is security.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009007|

4)Using IPSec:
IPSec is designed by Internet Engineering Task Force (IETF). It is a set of protocols between two devices across the network that provides data authentication and confidentiality using cryptography. It is a dominant VPN protocol. It provides cryptographic security to network traffics. Noteworthy features of IPSec are data origin authentication, confidentiality, anti-replay protection, perfect forward safety, dynamic re-keying, transparency.

IPSec works in two modes-transport modes and tunnel mode. In transport mode, all cryptographic operations are directly performed by both the source and destination hosts. The data is encrypted in the central and single tunnel with L2TP (Layer 2 Tunnelling Protocol). Whereas in tunnel mode cryptographic processing is performed by special gateways as well as the source and destination hosts. The encrypted data is sent through a series of tunnels created between gateways providing end-to-end security.
IPSec uses different protocols. But the two most frequently used protocols are
1)IPSec authentication header
Through this protocol, each packet is encoded with a digital signature to protect the data. The recipient verifies the authenticity of the packet.
2)Encapsulating security payload
ESP handles packet encryption by encrypting payloads for data.

IKE
IKE (Internet key exchange) is the protocol of IPSec which is used for secure communication between two devices. It operates on the Oakley protocol and ISAKMP (Internet Security Association and Key Management Protocol). It is used as a security for VPNs. Although IKE is not used as a configuration in IPSec it provides high range security.

A **public-key certificate** is a digital certificate that authenticates ownership. It is generated and issued by a trusted organization called a *certification authority*. To obtain a certificate from one requires identity proof. They bind the owner to the public. PKI encrypts the messages and data for security. It uses two sets of keys- a public key and a private key. The public key is available to any user who wants to verify the identity of the PKI holder whereas the private key is the secret key. Every digital certificate has a unique serial number for each certificate, algorithm information, name of the issuer, validate period i.e. the expiry date of the certificate, user name to whom the certificate belongs to and public key information.

III. CONCLUSION

Mobile IP has given a network mobility solution. Although, it has so many limitations. There are a large number of security threats. In this paper firstly we have discussed the working of mobile IP. Then we have investigated the security threats and have given some solutions to it. Mobile IP has a great scope. The security factor is the most important factor to be considered while studying mobile IP. Mobile IP can be secured with IPSec protocol. But there are some limitations. IPSec cannot stop traffic analysis, these limitations need to be studied. The use of public key adds to the security of mobile IP. Many mechanisms are used in mobile IP for security however solution to the security problems of mobile IP is a tough task. Thus, to make use of various techniques to solve the security issues of mobile IP is a research problem that needs to be solved urgently.

REFERENCES

1) Chandrasekaran, J. (2009). Mobile ip: Issues, challenges and solutions. *Newark: Rutgers University*.
2) Alkhawaja, A. R., & Sheibani, H. (2011). Security issues with Mobile IP.
3) Haitao'Zheng, W. The Security Issues and Countermeasures in Mobile IP.
4) Vachhani, M., & Ramani, P. (2013). Requirement of Mobile IP, its issues and solutions. In *IJCA (0975–8887) Proceedings on National Conference on Emerging Trends in Information & Communication Technology (NCETICT 2013)*.
5) Prasad, A., &Schoo, P. (2002). IP Security for Beyond 3G towards 4G. *Proceeding of WWRF, Eindhoven, Netherlands*.
6) Tuquerres, G., Salvador, M. R., &Sprenkels, R. (1999). Mobile IP: security & application. *Telematics Systems and Services*.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details