Security Overview of Mobile Internet Protocol

Zeeshan Hayat, Waqas Ahmad, Farid-ud-Din and Iqtidar Shah
Gandhara University of Sciences, Peshawer, Pakistan

Abstract– **The objective of this research paper is to endow with squat information to Mobile IP with impact/importance on the security aspects associated to it. A little scrutiny on Mobile IP introduction is provided, and the remainder of the paper is dedicated to IP authentication header, security tunneling, and Network Security model in campus intranets, sort of attacks and deployment of Mobile IP with security protection.**

Keywords– Overview, Security, Protocol and Analysis

I. INTRODUCTION

Mobile computing grants faultless, ever-present network access for mobile hosts like Laptop computers, Personal Digital Assistants and Electronic books.

Three practical entities, which define mobile IP:

1) Portable/Mobile Node: Node or workstation (laptop, Personal Digital Assistants) that be able to change its position in the Internet or intranet from one connection or network to another (distant link) Nevertheless utilizing merely its unique home Internet Protocol address which demonstrates what is the unique link for that node.

2) Residence Negotiator/Agent: A router or some gadget/device that has an interface on the mobile node's home network which espouses all the essential information/data of portable/mobile node.

- Portable/Mobile node grants of its contemporary location i.e. named (care of address) as the mobile/portable node shifts.

- Disrupt packets that are departing from the Portable/Mobile nodes dwelling/home address and burrow/tunnel them to the contemporary location of Portable/Mobile node; i.e. to the care of address.

3) Distant Negotiator/Agent: A tool/device or router on a Portable/Mobile node's tripped distant network which:

- assists the Portable/Mobile node to notify to its abode negotiator/home of its contemporary new care of address mostly specified by foreign agent from which home agent can locate precise position of the Portable/Mobile node.

- It propels/transmits a care of address and drive packets to the Portable/Mobile node that is launched actually tunneling through its residence agent; and

- It takes steps as chief interconnecting device for packets spawned through the Portable/Mobile node whilst hooked up to this foreign/distant network.

II. WORKING OF MOBILE INTERNET PROTOCOL

1) Residence negotiator/Agent and distant agents sporadically mingle their current links i.e. network address by multicasting or broadcasting through particular Mobile Internet Protocol announcement messages similar to NetBIOS messages, which are known as Agent Advertisement.

Mobile Internet Protocol is utilizing Agent Solicitation and Agent Advertisement, which are comparable to Internet Control Message Protocol router messages (RFC 1256).

2) Portable/Mobile nodes are relentlessly listening to these inward negotiator/agent Advertisements packets and interpret their contents to authenticate whether they are associated to their residence network link or a distant link. Even as linked to their residence connection Portable/Mobile nodes are active just like stationary nodes.

3) Care of address is specified by normally distant/foreign agent to the Portable/Mobile node that may possibly hook up to the distant network which is understandable from one of the header fields amongst the foreign/distant agent's Agent Advertisement packet.

4) Portable/Mobile node registers this address acquired in 3rd stage with its residence/Home agent through foreign agent, utilizing a message substitute mechanism cleared by Mobile Internet Protocol protocols. For evading remote denial-of service form of insider attacks, the registration messages techniques are obliged.

In favor of registration practice positive Registration demand/request message and Registration Reply message formats are utilized, that holds Internet Protocol header, User Datagram Protocol header and extensions.

5) In most cases it is the router on the residence network publishes attain capability to the network-address which will be discovered from the mobile node's home address. The residence agent acquires these packets through any Address Resolution Protocol mechanism, and transmitting them by mechanism of tunneling which is described in subsequent part to the care of address which is utilized for registration of Portable/Mobile node in stage/step 4.

6) On the care of address i.e. distant agent the inventive packet is recovered from the tunnel packets by de-encapsulating and then straightforwardly conveyed to the Portable/Mobile node, which is in identical network by express deliverance.

7) If mobile node desires for transmitting packets, at that time they are routed unswervingly to their destination entity,

devoid of visiting any foreign/distant agent or home/abode agent.

In general Internet Protocol tunneling is exercised when home/abode negotiator or agent throw packets to foreign/distant agent.

III. SECURITY

Authentication Header is to guarantee authentication/validation and truthfulness for Internet Protocol data gram packets and to grant fortification in opposition to replay assaults. It is effectively related to authentication/validation process.

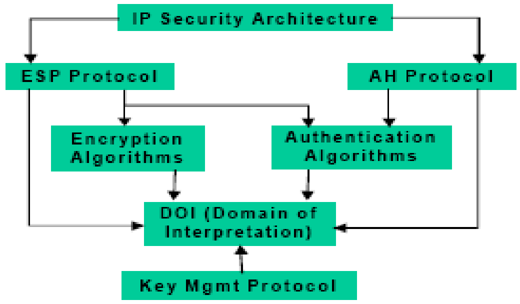
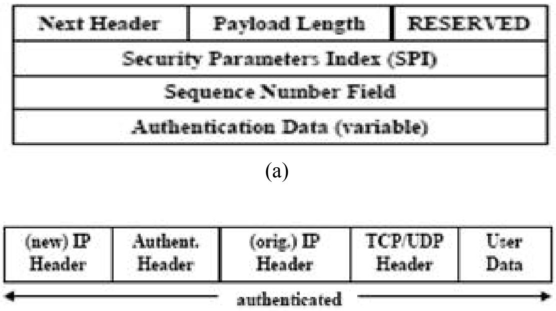


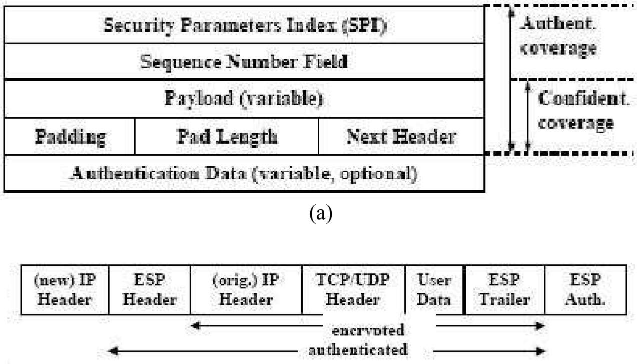
Fig. 1: Architecture of IP security



(a)

(b)

Fig. 2: (a) Format of AH, and (b) A Validate Tunneled Internet Protocol (v4) Packet



(a)

(b)

Fig. 3: (a) Internet Protocol sum up safety Payload Header, and (b) An Encrypted IPv4 Tunneled

Authentication Header protocol is dealt with diverse forms of algorithms, like (Message Digest), that constructs a data illustration that is 128 bit permanent size long and exclusive and it will be utilized for authentication/certification. There is a chain Number of 32-bit long field that indicates values utilized as counter that is exercised to bestow fortification from replay assault. The format of Internet Protocol Address Header is specified in Figure 2. The subsequent field is an 8-bit long that is exercised to recognize the kind of the subsequent payload. The Payload has length of 8-bit. There is a 6-bit reserved field for prospect reason exercise. The Security Parameter Index is 32-bit elongated value that indicates the Security Association for this datagram, which is distinctive. Authentication Data field as shown in figure 4 is variable length field and it has the Integrity Check Value (ICV). For better understanding, Fig. 2 also exemplifies how an authenticated/validated packet format will revolutionize in tunneling. ESP pacts with dissimilar authentication/certification and encryption algorithms and fig 3 show the use of the DES-CBC transform. Once packet is encrypted, only certified and authorized clients may possibly decrypt it.

The Internet Key Exchange (IKE) method or protocol is utilized to switch over or to negotiate some imperative parameters and confirm keys flanked by two communicating nodes and the association of a Security Associations. It is a one sided conformity involving two entities. Fig. 4 shows the table of SA.

There are diverse varieties of firewalls subsists for safe and sound communication.

By and large, it is putted into practice in security gateways. The largest sophisticated and vital part for mobile/portable Internet Protocol employed as a firewall that is called as secure tunneler, which is as shown in Fig. 5. This firewall is utilizing Address Header and ESP protocols stated above.

Security Parameter Index	Authent. algorithm	Authent. key	Replay protection	Encryption algorithm	Encryption key
01234567	e.g., Keyed MD$	(a secret key)	timestamp		
89ABCDEF				e.g., RSA	(public/ private key)

Fig. 4: Security Associations

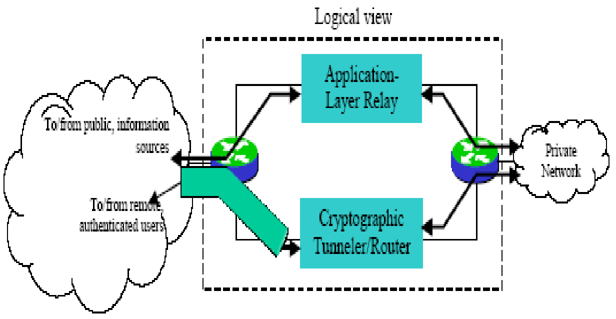

Logical view
Application-Layer Relay
Cryptographic Tunneler/Router
To/from public, information sources
To/from remote authenticated users
Private Network

Fig. 5: Safe and sound Tunneler

IV. CAMPUS INTRANET

We are taking campus intranet as sanctuary/security sculpt/model to be conscious of unusual things of Mobile/portable Internet Protocol assaults and protection. In this part we are bringing into play the network defense/security model shown in Figure 6. We ought to build some conjectures be fond of a network having no links to the Internet, and no firewalls installed wherever with protected entrée.

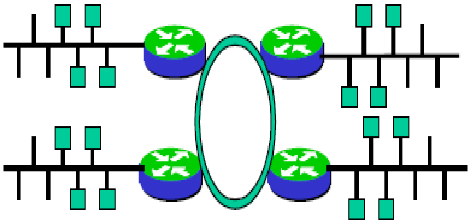


Fig. 6: A Network sculpt for Mobile/portable Internet Protocol in campus intranet

Mobile/portable nodes and network itself are relatively susceptible/at risk to assault from insiders in numerous cases they are own/possess employees of the company, and carry out the malevolent functions/purposes/tasks.

A. Service Denial

Denial of service is an attacker precluding a justifiable node from being paid some work done. There are two forms of denial of service: A bad guy throws and accomplish flooding to a host i.e. averting that host/user from dealing out/processing his concern packets. A denial of service assault can occur when an assailant someway administers to do a erroneous or proxy registration request of a new care of address for a fastidious legitimate node and got registered. It will generate following two nuisances.

- Mobile/portable node, good guy cut off from all communications, In view of the fact that it cannot entertain any sort of packets.
- Bad guys can notice a replica of all packets of the inventive mobile node.

How assailant will perform this is shown in Fig. 7.

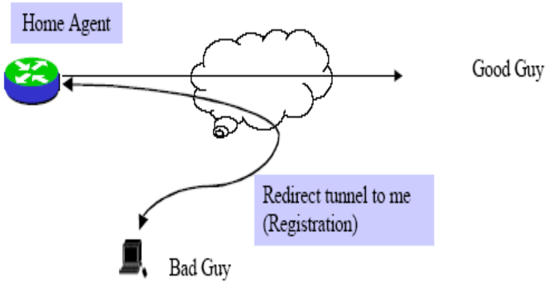


Fig. 7: Denial of Service Assault

Mobile/portable Internet Protocol specification/plans discontinue bad guys/hackers from constructing a counterfeit registration. This kind of assault impracticable, under postulation that the secret key will not be out of order. A further form of denial of service assault is recognized as replay attack that is alike in equally ways. When the assailant maps out the encrypted registration request, which is transmitted by mobile/portable node, assailant obstructs that message and replays that message after some time. There are two strides/steps to shun/avoid replay assaults: (1) in initial type the ID field in the message format is filled by timestamp or whichever nonce value. (2) After nonce is utilized a particular value is taken into account which ought to be acknowledged by equally the communicating parties; so even if the assailant recognizes what that concern value in various ways but he won't be capable to craft any harm.

B. Eavesdropping

It is contrary to the vigorous assaults that we confer so far. This assault transpires when an assailant listens or captures packets swapped between home/residence agent and good guy mobile/portable node. So this is associated/linked to confidentiality/privacy. Assailants can entrées to the traffic by breaching router password or any connection. For wireless network it is very tough to formulate harmless the radio signals for any assailant. To restrain radio signals is not a gigantic charge. To avert this assault it is obligatory to encrypt information while transmitting and is very essential having wireless networks. Packets ought to be encrypted aforementioned to transmitting and it can be through by diverse schemes as conferred in subsequent section. The finest clarification for inactive eavesdropping is end to end encryption of each and every packet. A bad guy that eavesdrops at any position of the exchange is the subsequent panel of the figure 8 will observe only encrypted text that he is not satisfactorily connoisseur of decrypting if he don't identify key. Commonly we are bringing into play digest schemes after that it is impractical to interpret this sort of data by seize it.

Several examples that utilize end-to-end encryption are SSH (Secure remote (UNIX) Shell), SSL (Secure Socket Layer) ands (Secure remote file Copy). This encrypts not merely the application layer data and protocol header but the transport layer header as well, which will thwart a bad guy from determining which application is being sprint/run, Permit alone the data exchanged as part of that application.

C. Pilfering/burglary of Session

It is a vigorous form of information theft. To craft this capable following steps are followed:

- Bad guy dangles in relation to till the genuine node begins registration practice in the direction of its home/residence negotiator/agent;
- Bad guy may possibly be in prospect to eavesdrops to keeps an eye on the exchange if the mobile/portable node is performing some imperative data transmit or communication
- Afterwards the assailant surplus the mobile/portable node with nuisance, by busying it with meaningless task.

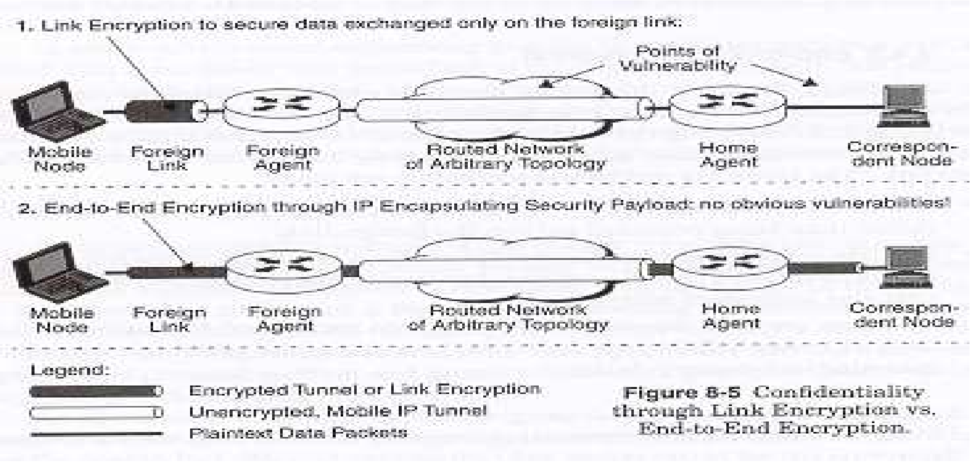

1. Link Encryption to secure data exchanged only on the foreign link:
Points of Vulnerability
Mobile Node
Foreign Link
Foreign Agent
Routed Network of Arbitrary Topology
Home Agent
Correspon-dent Node
2. End-to-End Encryption through IP Encapsulating Security Payload: no obvious vulnerabilities!
Mobile Node
Foreign Link
Foreign Agent
Routed Network of Arbitrary Topology
Home Agent
Correspon-dent Node
Legend:
Encrypted Tunnel or Link Encryption
Unencrypted, Mobile IP Tunnel
Plaintext Data Packets
Figure 8-5 Confidentiality through Link Encryption vs. End-to-End Encryption.

Fig. 8: End-to End Encryption and Link Encryption (Confidentiality)

- Bad guy may possibly conquest the session by forthcoming packet and concurrently by listening packets departing towards the mobile node.

Mobile/portable node (good guy) may possibly befall conscious that something is not right because his applications will discontinue execution, but he may not acquire that his sessions have been seized. The guard against session stealing assaults is also cryptography, which is practical in inactive/passive eavesdropping. By encrypting the traffic on as shown in Figure 8 (preferably everywhere on the connection- end to end encryption), so assailant thrived in pilfering session but he will not be in the position to decrypt the real data.

D. Other Energetic/Vigorous Attacks

Vigorous/active assaults will scrutinize in which Bad Guy construct admittance to network jack, acquire an Internet Protocol address and utilizing them attempts to go into the further host's workstation on the network. The procedure to be tagged all along after the assailant achieves the right to draw on over the network

- Bad guy investigate a network prefix that is interrelated to the link to which the network jacks are associated. Capturing mobile/portable Internet Protocol agent advertisement packets, by hauling out and examining, does this IP addresses in packets or even by just manufacturing a Dynamic Host Configuration Protocol request, which is straightforward UDP packet.
- Bad guy may possibly strive to guess some host number indiscriminately to exploit for subsequent assault, which can be done by bearing in mind the Address Resolution Protocol request and ensure if they are unanswered. Then there is a fine possibility to that the chosen host number is not being utilized.
- Once any of above steps accomplished the assailant initiates to connect IP hosts. This is feasible by guessing administrators are not cautious to opt for username and password.

To thwart vigorous assaults, these two feats have to be carrying out:

(1) The 'R' bit ought to be forced to all the publicly reachable points compulsorily. So, all communicating mobile/portable nodes have to carry out process for permissible registration with the foreign/distant agent whether it is aggressor or good guy.

(2) Second data link layer encryption or end-to-end encryption ought to be compulsory for all mobile nodes in network who would like to connect to the foreign/distant agent whenever they visit new network or link.

V. MOBILE IP ALL-INCLUSIVE

Here security/defense threats of the intranet discussed above also included the vision with assault to the scrupulous mobile node, which is outer surface of the intranet i.e. in public network. So protection for mobile node as well as how this mobile node accesses the intranet in protected manner is discussed in this section. We will then argue the problem of mobile nodes entertaining packets after fleeting the firewall and they are positioned remotely to the private network i.e., anywhere in public network or Internet.

A. Wide-reached/Internet Mobility exploitation

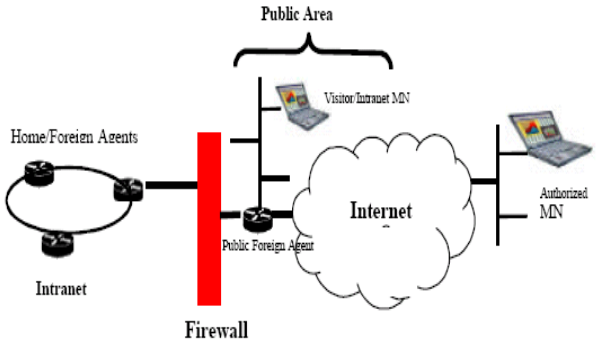


Fig. 9: Mobile IP employment scenario

In Fig. 9 all the data is fleeting through the firewall. The home/residence agents are sheltered by the firewall but it is not promising all foreign agents cannot be under the protection of firewall. Therefore these agents can shore up unreceptive or vigorous eavesdropping.

B. Protection

Now in general all workstations have firewall software. Fig. 10 depicts the exploitation of Virtual Private Networks for defending Intranets. A VPN is the amalgamation of two or more substantial/physical private networks that are looking like connected but in point of fact separated by a public network like Internet and from the user's view they behaves as a single private network. The firewall grants protection to its network by declaring and allowing only those packets those are fittingly authenticated/certified and encrypted by another end firewall.

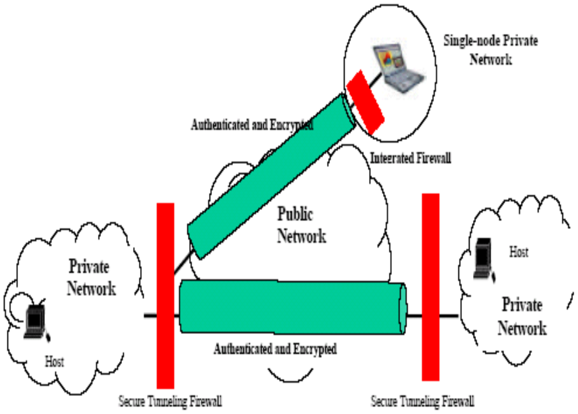

Single-node Private Network
Authenticated and Encrypted
Integrated Firewall
Public Network
Private Network
Host
Host
Private Network
Authenticated and Encrypted
Secure Tunneling Firewall
Secure Tunneling Firewall

Fig. 10: VPN ensuring secure firewall

In the Fig. 10, mobile node communicating through safe and sound tunneled. We know that the secure tunneled is worked as a firewall as shown in Fig. 7 that provides a cryptographically-protected path only for authorized users to use a private network by passing through public network. Simple Key-Management protocol (SKIP) [3] is method and solution of the method to traverse or pass the firewall securely as shown in Fig. 10.

VI. CONCLUSION

Initially, we acquired a little preface about Mobile/portable Internet Protocol and then conferred the scrutiny of security/protection in mobile IP in straightforward campus Intranet network protection sculpt and in the Internet also. We acquired a fleeting glance of the AH, ESP and the IKE protocols according to the IETF's IPSec architecture. We obtained evaluation of odd types of assaults similar to denial of service, passive/inactive eavesdropping, session stealing and other active/vigorous attacks etc. In campus intranets and possible protection against them. The make use of the safe and sound tunneled is a crucial and key protection mechanism was explained here. We also acquired up to some extent about certification and encryption techniques to put off security assault. Major 3 objectives of network sanctuary ought to be conserved. The common way out can be formulated utilizing tunneling with authentication and encryption between the firewall and mobile node. Providing confidentiality, authentication and integrity all the way through the Internet by using security mechanisms, services and protocols with are under embellishment and research by the IETF. The research will also wrap IPv6 and ranges from the data link layer up to the application layer.

REFERENCES

[1] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 2406, November 1998.

[2] G. Montenegro and V. Gupta. SKIP Firewall Traversal for Mobile IP of Sun. RFC 2356, June 1998.

[3] C. Madison and R. Glenn. The Use of HMAC-MD5-96 within ESP and AH. RFC 2403.

[4] AAA and Network Security for Mobile Access by Madjid Nakhjiri and Mahsa Nakhjiri- Wiley Publication.

[5] J. D. Solomon. Mobile IP - The Internet Unplugged. Prentice-Hall, 1997.

[6] http://www.europe.cisco.com/univercd/cc/td/doc/product/access/mar_3200/mar_conf/m516secu.htm

[7] MOBILE IP: SECURITY & APPLICATION – a research paper by Gloria Tuquerres, MarcosRogério Salvador and Ron Sprenkels at the University of Twente, The Netherlands.

[8] http://ieeexplore.ieee.org/iel5/7020/18920/00874016.pdf

[9] http://www.tcpipguide.com/free/t_MobileIPSecurityConsiderations.htm