Mobile IP Working Group
INTERNET DRAFT

V. Gupta
SUN Microsystems
S. Glass
FTP Software
March 17, 1997

Firewall Traversal for Mobile IP: Guidelines for Firewalls and Mobile IP entities

draft-ietf-mobileip-firewall-trav-00.txt

Status of this Memo

Abstract

The use of network security mechanisms such as ingress filtering, firewall systems and private address spaces can disrupt normal operation of Mobile IP [GuGl97]. This document outlines behavioral guidelines for Mobile Nodes, their Home Agents and intervening Firewalls. Compliance with these guidelines allows secure datagram exchange between a mobile node and its home agent even across firewalls, ingress filtering routers and distinct address spaces. To its correspondent nodes, the mobile node appears to be connected to its home network even while roaming on the general Internet. It enjoys the same connectivity (modulo performance penalities) and, if

desired, privacy outside its protected domain as on the inside.

The guidelines described here solve a restricted, but still useful, variant of the general firewall traversal problem for Mobile IP. They make the following assumptions: (a) All intervening firewalls belong to the mobile node's protected home domain and their existence and relative placement, with respect to a mobile node's current location, is known a priori. (b) Mobile nodes use co-located care-of addresses (rather than Foreign Agents) when outside their protected home domain. (c) Firewalls implement standard protocols for authentication and encryption [RFCs 1825, 1826, 1827] but need not understand Mobile IP message formats. (d) When private addresses are used inside a Mobile node's home domain, the home agent is able to distinguish between private and public addresses.

1. Introduction

The IETF Mobile IP protocol [Per96a] allows a mobile node (MN) to continue sending and receiving IP datagrams using a fixed address, its home address, even when it is no longer connected to its home subnet. When a mobile node visits a foreign subnet, it obtains a care-of address on that network and registers that address with its home agent (HA), a special entity residing on its home subnet. The home agent, in turn, intercepts datagrams meant for the mobile node and tunnels them to the registered care-of address. Tunneling refers to the process of enclosing the original datagram, as data, inside another datagram with a new IP header [Per96b, Per96c]. The new header carries the mobile node's care-of address in the destination field. The care-of address may belong to a specially designated node -- the foreign agent (FA) -- or may be a temporary address assigned to one of the interfaces of the mobile node, e.g. through DHCP or PPP. In the latter case, the mobile node is said to have a co-located care-of address. This mode of operation obviates the need for explicit mobility support, in the form of an FA, on the foreign subnet, though local policy may still require a mobile node to register through an FA. The recipient of a tunneled packet recovers the original datagram before processing it further.

Mobile IP assumes that routing of unicast traffic is based solely on the destination address. Many Internet routers now include other considerations in their forwarding decision, e.g. in an effort to guard against IP-spoofing attacks, source-filtering routers drop datagrams that arrive on an interface inconsistent with their source address [CA9621]. Such a router, if present on the foreign network, will block all datagrams generated by a visiting mobile node carrying its home address as source. A solution to this problem is to use a reverse tunnel directed from the mobile node's care-of address to its home agent [Mont97]. Under this arrangement, datagrams sent from MN

to a correspondent node (CN) now carry the care-of address (rather than the home address) as source in the outermost IP header and pass unchallenged through source-filtering routers to the mobile node's home agent. The home agent strips the outer IP header and recovers the original packet. From then on, the packet is forwarded as if the mobile node were on its home subnet.

Additionally, many organizations use firewalls to protect their networks from the general Internet. These firewalls impose additional constraints, e.g. they may drop unsolicited datagrams from untrusted external hosts [ChZw95]. Such a policy is enforced by carefully screening the source and destination addresses, as well as ports, on all transport level packets. For TCP packets, the firewall may also monitor the ACK bit. In this situation, a mobile node's registration requests are likely to be dropped by a firewall protecting its home network. Note that source-filtering is not an issue here because registration requests arrive with a topologically correct source address - namely the current care-of address of the mobile node.

To complicate matters, organizations often hide the topology of their internal network by using private addresses. These addresses are not advertised to the general Internet. Such addresses include, but are not restricted to, those defined in RFC 1918. The Internet's routing fabric is unable to route packets to these addresses (resulting in ICMP unreachables). To allow connections from the internal network to the general Internet, application relays (also called application gateways or proxies) are used. In a typical configuration, the internal network is separated from the general Internet by a "perimeter network" on which the firewall and proxies are located [ChZw95] (see Figure 1). Hosts on the peripheral network use public addresses, i.e. their addresses are advertised to the general Internet. When a host on the internal network wishes to connect to the Internet, two separate connections are set up: one between the internal host and the proxy and another between the proxy and the outside host. To the external host, the user at the other end appears to be on the proxy host.

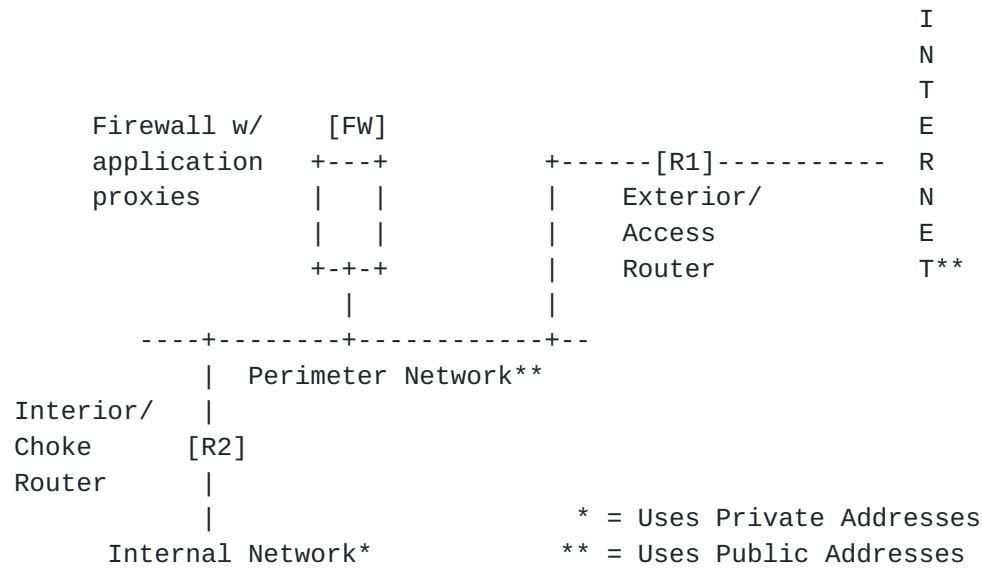


Figure 1: Screened-subnet firewall architecture.

The use of private addresses on firewall-protected networks poses an additional challenge. A mobile node belonging to such a network can not use its home address (a private address) to communicate directly with correspondent nodes when it is outside the protected domain since replies from correspondent nodes to the private address will likely generate a "host unreachable" ICMP message. If, somehow, a reverse tunnel can be established from the mobile node to its home agent, the mobile node can continue using its private home address. Datagrams generated by the mobile node using its home address will appear to emerge from its home network and connections to external hosts will still involve an intermediate proxy.

The presence of intermediate firewall(s) disrupts free flow of packets from a mobile node on the outside to its home agent on the inside. In its current form, this draft provides a conceptual framework for achieving the required connectivity by mutual cooperation between mobile nodes, their home agents and intervening firewalls. As proposed IPSEC standards stabilize, later revisions will incorporate greater details, e.g. message formats required to establish dynamic security associations.

2. Solution Overview

In a security-conscious environment, there are two main obstacles preventing free flow of datagrams between a mobile node and its home agent. Both can be countered as described below:

(1) Firewalls: Their main purpose is enforcing controlled access to the internal network. Firewalls can use IPSEC authentication to establish the true identity of a datagram source. Their security policy can be appropriately configured such that packets between an authenticated mobile node and its home agent are allowed to pass.

Additionally, IPSEC encryption can be used between the outermost (perimeter) firewall and the mobile node to keep untrusted hosts, outside the protected domain, from prying on a mobile node's traffic.

(2) Ingress Filtering/private address spaces: We group these together because both mechanisms are implemented by filtering routers. These routers do not forward any datagram in which either:

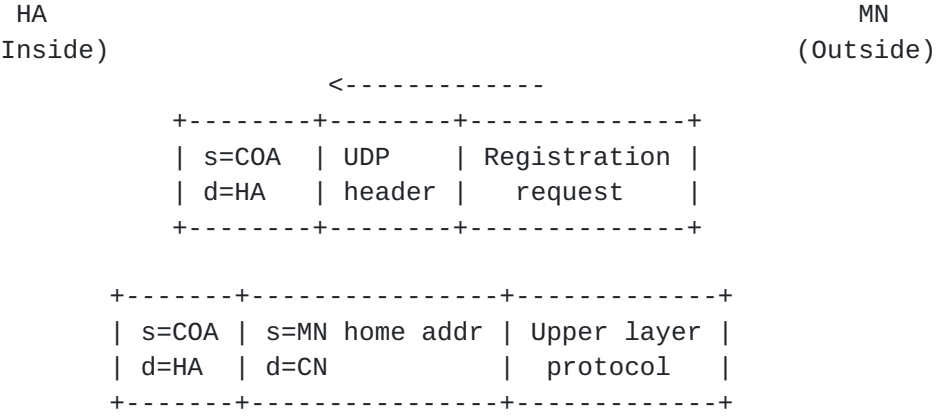
(i) The source address is inconsistent with the interface that the datagram arrives on, i.e. the source is topologically incorrect. Note that an unknown source addresses can be thought of as always being topologically incorrect.

(ii) The destination address is unknown.

These routers can be countered by using (possibly multiple levels of) tunneling such that on the outermost IP header both the source and destination addresses are known to the router and the source address is topologically correct.

There are only two kinds of datagrams that need to pass back and forth through these obstacles:

(a) Datagrams directed from a mobile node to its home agent which include registration requests and reverse tunneled traffic. In either case, the (outermost) IP header contains the mobile node's care-of address (COA) as source and the home agent's address (HA) as destination.



For the rest of this article we represent both of these as follows and refer to it as an "inbound" packet.

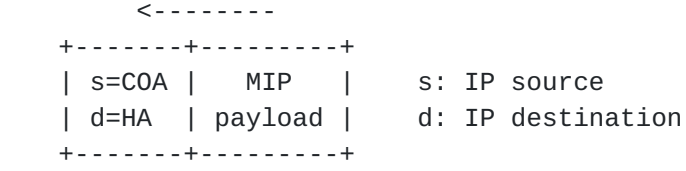
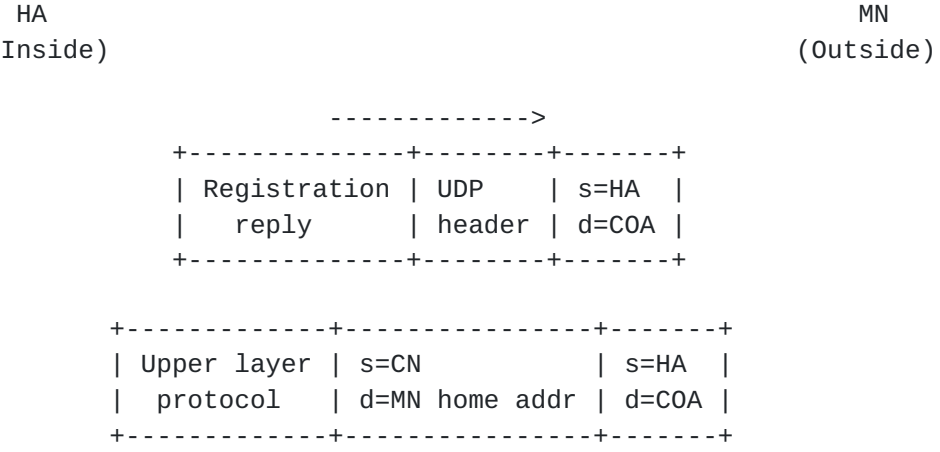


Figure 1: Inbound packet

(b) Datagrams directed from a home agent to a mobile node which include registration replies and (forward) tunneled traffic. In either case, the (outermost) IP header contains the home agent's address as source and the mobile node's care-of address as destination.



For the rest of this article we represent both of these as follows and refer to it as an "outbound" packet.

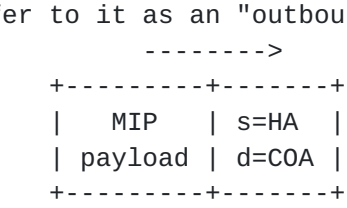


Figure 2: Outbound packet

2.1 Assumptions

Our solution is based on the following assumptions:

(a) A mobile node can deduce its current location and the sequence of firewalls that must be traversed to reach the home agent. The exact mechanism for doing so is unspecified and will primarily be decided by the local (home) security policy. It may be based on manual pre-configuration, user input or a separate dynamic firewall-discovery protocol. Such a discovery protocol is beyond the scope of this document. For the rest of this article we label the intervening firewalls FW1, FW2, ..FWn. Here, FW1 is the perimeter firewall guarding the home domain from the Internet.

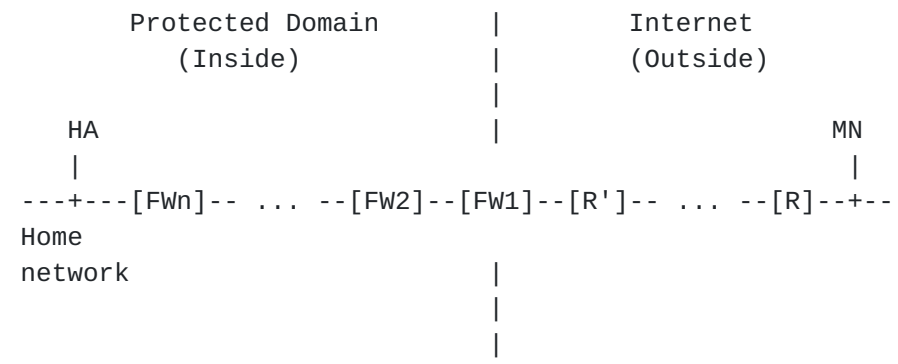


Figure 3: Security framework addressed by this document.

(b) All firewalls are IPSEC-aware and able to establish security associations between themselves.

(c) FW1 is the only firewall whose address is advertised on the general Internet, i.e. routers such as R and R' can route packets to FW1 but are not aware of the addresses used internally by FW2, ... FWn. In contrast, routers on the inside are able to route packets for FW1 through FWn but are unaware of any addresses used on the outside Internet.

(d) Any number of routers may exist between the MN (outside the home domain), and HA (inside the home domain), any or all of which implement source filtering, i.e. they drop packets on which the source address is either unknown or inconsistent with the interface on which the datagram is received. All routers drop packets meant for unknown destinations.

(e) The Mobile Node is IPSEC aware and can acquire an appropriate security association with each firewall such that packets authenticated with that association are allowed to pass through. This acquisition may either be based on manual configuration or a key management and distribution protocol [MSST96, Orma96].

(f) When MN is outside the protected domain, there are no firewalls between it and FW1.

(g) Nodes within the protected domain trust each other, so, for example, there is no need to encrypt a mobile node's traffic on network links inside the protected domain. Note that procedures defined in this document do not preclude end-to-end or other forms of such encryption, should they be required by an organization's security policy.

(h) A home agent belonging to the protected domain is able to distinguish between addresses belonging to the protected domain

and those on the outside. Manual configuration is one option (e.g. one could supply a list of "internal addresses" and all others will be treated as "external). It is also possible to introduce a new MN-HA extension in registration requests that identifies the care-of address as being "external". This essentially transfers the burden of identification from the HA to the MN which may be justified since the latter can consult the user if needed.

Note that assumptions (c) and (d) represent additional constraints accommodated by our solution rather than solution requirements.

3. Inbound Datagram Processing

On realizing that it is outside its protected domain, a mobile node first establishes a security association with the perimeter firewall. IPSEC compliant key management protocols must allow separation between an entity's true identity and its current IP address. This distinction is crucial for a mobile node when it must send a packet with its current care-of address past a firewall. If necessary, this exchange may have to be repeated for each of the other firewalls in sequence. To send an "inbound" packet to its home agent, the mobile node prepends a tunnel mode authentication header for each firewall starting with FWn. In addition, transport mode encryption may (optionally) be inserted before prepending the authentication header corresponding to FW1. If both authentication and encryption are desired between the mobile node and FW1, the mobile node may choose a single ESP transform that accommodates both.

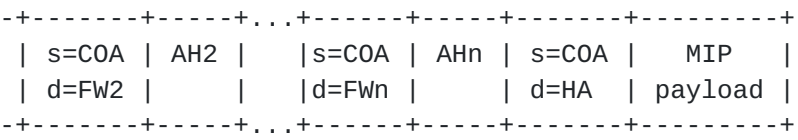


Figure 4: An "inbound" packet as it leaves the mobile node.

The security policy on each firewall should be configured to processes packets as follows:

(a) Look for an authentication header in the datagram (drop packet if there isn't one) and look up the security association referenced by the included Security Parameter Index [RFC1825, 1826].

(b) Verify the authenticator (drop packet if authentication fails).

(c) Decrypt packet if ESP is present to recover a new datagram. Note that steps (b) and (c) may need to be performed multiple times if there are nested security headers for the same destination. This process will eventually yield a datagram to be forwarded beyond this firewall.

(d) If the last exposed datagram is likely to be dropped by filtering routers before reaching its destination (e.g. because the source address is unknown), then tunnel the packet of item (c) to the next destination. Either a tunnel-mode IP Authentication Header or plain IPinIP may be used since both are able to hide the unknown source address (COA) from internal routers.

Actions (a)-(c) do not place any additional burden on IPSEC compliant hosts. Action (d) is required only if the protected domain uses private addresses and internal routers are configured to drop packets in which the source or destination address is unknown or the source is inconsistent with the interface on which the packet arrives. Even so, action (d) may not be required at all firewalls, e.g. FWn can skip this step if there are no filtering routers between FWn and HA.

As a result of these actions, the "inbound" datagram datagram looks as follows as it travels towards the home agent.

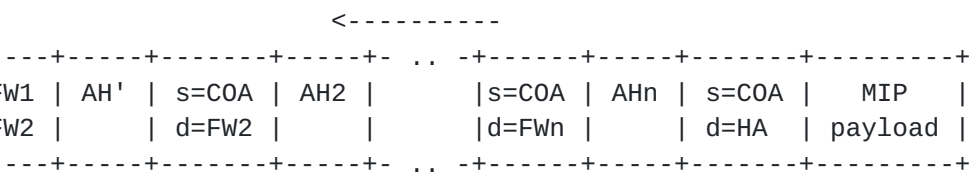


Figure 5: "Inbound" packet on its way from FW1 to FW2.

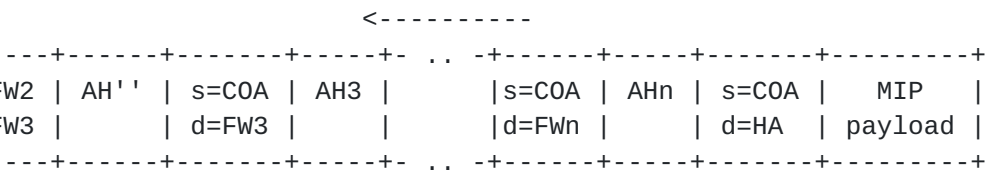


Figure 6: "Inbound" packet on its way from FW2 to FW3.

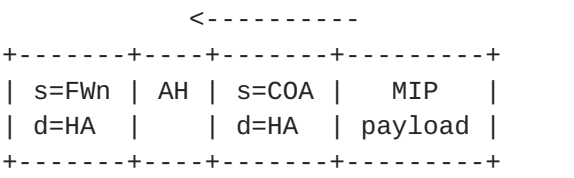


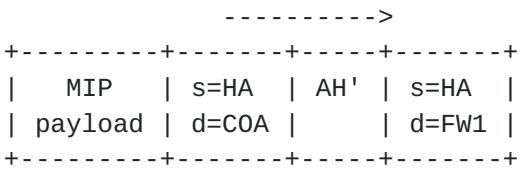
Figure 7: "Inbound" packet on its way from FWn to HA.

The home agent recovers the original "inbound" packet (Figure 1) and processes it as under normal Mobile IP (in the presence of reverse tunneling [Mont97]). Note that depending on the kind of tunneling used in step (d) and the placement of filtering routers, HA may need to be IPSEC aware.

4. Outbound Datagram Processing

Since hosts inside the protected domain are trusted, non-perimeter firewalls like FW2, ..., FWn may be configured to allow outgoing packets to pass without any authentication. In this situation, outbound datagram processing is quite simple.

The home agent creates an outbound packet as part of normal Mobile IP operation. If the destination is recognized as being outside the protected domain, the packet is explicitly directed at the perimeter firewall FW1 either by using IPinIP tunneling or a tunnel mode Authentication header. The former requires that FW1 be able to decapsulate IPinIP datagrams while the latter requires HA to be IPSEC aware. The resulting packet is shown in Figure 8.



MIP payload	s=HA d=COA	AH'	s=HA d=FW1

Figure 8: Outbound packet as it leaves HA (the authentication header may not be needed).

Once this packet reaches the perimeter firewall FW1 successfully, the original "outbound" datagram is recovered (either after IPSEC processing or IPinIP decapsulation).

The security policy on FW1 must be configured as follows: If a packet is to be forwarded to a destination for which a security association exists, appropriate IPSEC headers must be added before forwarding.

As a result of this policy, the "outbound" packet looks as shown in Figure 9 as it leaves FW1 for the mobile node.

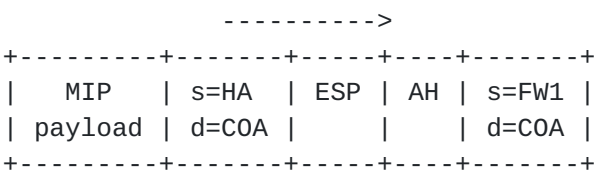


Figure 9: "Outbound" packet on its way from FW1 to MN.

Intermediate routers such as R' and R'' see a topologically correct source address and a routable (known) destination address. Once the packet reaches the mobile node, the original "outbound" datagram is recovered after IPSEC processing and processed as with normal Mobile IP.

If FW2, ... FWn require source authentication even on outgoing packets the process by which the outbound datagram reaches FW1 is no longer as simple. In this situation the overall processing is similar to that described for inbound datagrams but in the reverse direction.

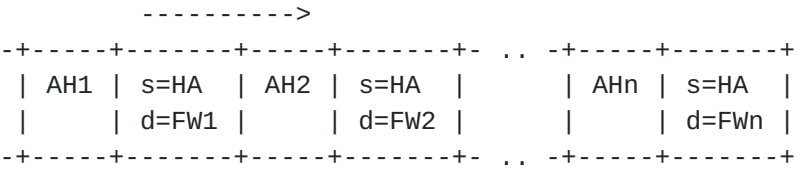


Figure 10: An "outbound" packet as it leaves HA.

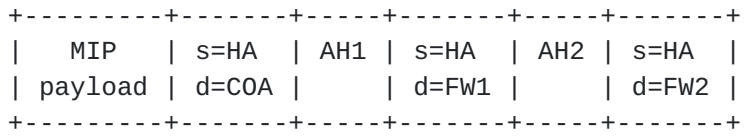


Figure 11: An "outbound" packet on its way from FW3 to FW2.

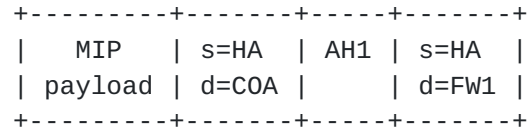


Figure 12: An "outbound" packet on its way from FW2 to FW1.

Note that intermediate firewalls do not need to prepend additional headers before forwarding an outbound packet because already the outermost source and destination are known to internal routers and the source is topologically correct.

5. Closing Remarks

The mechanism outlined here allows Mobile IP operation even when a mobile node roams outside its firewall-protected domain. This functionality is achieved at the cost of introducing sub-optimal "quadrangle" routing and additional header overhead. The amount of header overhead depends on the number of intervening firewalls. In most cases just a single firewall must be traversed. Preliminary experiments on a SKIP-based implementation [MoGu96] suggest that the performance penalty due to IPSEC processing and additional headers on sustained throughput is roughly ten percent. Bursty traffic rates can show significant variance because the use of Mobile IP and IPSEC tunnels delays Path MTU discovery. Several packets may need to be sent before the sender's path MTU estimate becomes small enough to account for all intermediate tunnels, e.g. one ftp transfer of a 0.5 MB file attained a transfer rate of 7KB/s but after the path MTU had been cached at the sender, the same file was transferred at a rate of 270 KB/s.

6. Security Considerations

This entire document discusses security considerations for mobile nodes. Using the procedure outlined in this document, datagrams between a mobile node and its home agent can pass freely through firewalls protecting its home domain. In this situation, the mobile node acts as an extension of the security perimeter surrounding its home domain and must, therefore, share in the responsibility of protecting it from outsiders. In the absence of user-specific keying information, someone who steals the mobile node may also gain access to the home network.

Acknowledgments

This document builds upon ideas previously introduced in [MoGu96] and discussions at the "Secure firewall Traversal for Mobile IP" special meeting held during the 37th IETF meeting.

References

[CA9621] CERT Advisory CA-96.21, "TCP SYN Flooding and IP Spoofing Attacks", available at ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding.

[ChZw95] D. B. Chapman and E. Zwicky, "Building Internet Firewalls", O'Reilly & Associates, Inc., Sept. 1995.

[GuGl97] V. Gupta and S. Glass, "Firewall traversal for Mobile IP: Goals and Requirements". Draft <draft-ietf-mobileip-ft-req-00.txt> -- work in progress, January 1997.

[LGLK96] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas and L. Jones, "SOCKS Protocol Version 5", RFC 1928, March 1996.

[Leec96] M. Leech, "Username/Password Authentication for SOCKS V5", RFC 1929, March 1996.

[MSST96] D. Maughan, M. Schertler, M. Schneider and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", version 7, Draft <draft-ietf-ipsec-isakmp-07.{ps,txt}> -- work in progress.

[McMa96] P. McMahon, "GSS-API Authentication Method for SOCKS Version 5", RFC 1961, June 1996.

[Mont97] G. Montenegro, "Bi-directional Tunneling for Mobile IP", Draft <draft-ietf-mobileip-tunnel-reverse-00.txt> -- work in progress, Feb. 1997.

[MoGu96] G. Montenegro and V. Gupta, "Firewall Support for Mobile IP". Draft <draft-montenegro-firewall-sup-00.txt>, work in progress, Sept. 1996.

[Orma96] H. Orman, "The Oakley Key Determination Protocol", version 1, Draft <draft-ietf-ipsec-oakley-01.txt> -- work in progress.

[Per96a] C. Perkins, "IP Mobility Support", RFC 2002.

[Per96b] C. Perkins, "IP Encapsulation within IP", RFC 2003.

[Per96c] C. Perkins, "Minimal Encapsulation within IP", RFC 2004.

Author's Address

Vipul Gupta
Sun Microsystems, Inc.
2550 Garcia Avenue
Mailstop UMPK 15-214
Mountain View, CA 94043-1100

Tel: (415) 786 3614
Fax: (415) 786 6445

EMail: vipul.gupta@eng.sun.com

Steven M. Glass
FTP Software
2 High Street
North Andover, MA 01949

Tel: (508) 685 4000
Fax: (508) 684 6105

EMail: glass@ftp.com