John K. Zao, BBN Technologies
Matt Condell, BBN Technologies

Use of IPSec in Mobile IP

Status of this Memo

Abstract

The use of IPSec ESP protocol in the Mobile IP packet redirection tunnels will protect the redirected packets against both passive and active attacks launched and aid these packets to traverse the firewalls surrounding both the home and the foreign subnets visited by the mobile nodes.

This document proposes a scheme to negotiate the use of IPSec ESP on selected Mobile IP tunnels and a procedure to establish these tunnels with the aid of automatic key and security association management protocol such as ISAKMP.

Table of Contents

1. Introduction....3
2. Security Requirements of Mobile IP....4
2.1 Security Requirements of Mobile Nodes....4
2.1.1 Connectivity Protection between Mobile Nodes and Home Subnets....4
2.1.2 Connectivity Protection between Mobile Nodes and Other Subnets...5
2.2 Security Requirements of Visiting Subnets....5
2.2.1 Protection of Network Resources....6
2.2.2 Protection of Local Traffic....6
3. Use of IPSec on Mobile IP Redirection Tunnels....6
3.1 Operation Principles....6
3.2 Choice of IPSec Protected Mobile IP Tunnels....7
3.2.1 MN-HA Tunnels....9
3.2.2 HA-FA Tunnels....9
3.2.3 MN-FA Tunnels....10
4. Changes to Mobile IP Messages....10
4.1 Extension to Mobility Agent Advertisement....10
4.2 Extension to Mobile IP Registration Request....11
4.3 Mobile IP Registration Reply....12
5. Procedure for MIP-IPSec Tunnel Establishment....12
5.1 Selection of MIP-IPSec Tunnels....12
5.2 Negotiation of Security Associations and Keys....13
5.3 Activation of MIP-IPSec Tunnels....13
6. Format of Encapsulated Packets....14
7. References....14
Disclaimer....15
Author Information....15

1. Introduction

IP mobility support or Mobile IP [rfc2002] enables a mobile node to change its attachment point on the Internet while maintaining its IP address(es) as well as its network connectivity using these IP addresses. The protocol permits mobile internetworking to be done on the network layer; however, it also introduces new vulnerabilities to the global internet, most notably:

1. the possibility for an adverse node to spoof the identity of a mobile node and redirect the packets destined for the mobile node to other network locations,

2. the risks for potentially hostile nodes (coming from different network administrative domains) to launch passive/active attacks against one another when they use common network resources and services offered by a mobility supporting subnet.

The first type of vulnerability can be surmounted by the strong authentication mechanisms built into both basic Mobile IP [rfc2002] and route optimized Mobile IP [mip-optim]. With the aid of a public key infrastructure [moips], a scaleable countermeasure against the spoofing attack can readily be deployed. In contrast, the second type of vulnerability was left largely unattended. This Internet Draft proposes a scheme to apply IP security protocol [ipsec-arch] onto the IP-IP encapsulation used by Mobile IP to redirect IP datagrams to and from the mobile nodes. The purpose is to provide authentication and confidentiality services to Mobile IP redirection traffics in order to protect them against passive and active attacks and to help them pass through security gateways.

The proposed scheme includes

1. a mechanism for negotiating the use of IPSec protection on selected Mobile IP redirection tunnels,
2. a procedure for establishing these IPSec protected tunnels and
3. the formats of tunneled packets in either full IP-IP or minimal IP-IP encapsulations.

In the next two sections, we will first study the security services that are needed to counter the second vulnerability of mobile internetworking, and the different IPSec tunnels that can be set up in the context of Mobile IP. Then, we will describe the three parts of the proposed scheme in separate sections.

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this

document, are to be interpreted as described in RFC 2119 [rfc2119].

2. Security Requirements of Mobile IP

The security requirements of mobile internetworking should be considered from two perspectives: (1) the expectation of the mobile nodes to retain their network services and protect their communication when they visit the foreign subnets and (2) the expectation of the foreign subnets to protect their network resources and local traffic while they are visited by the mobile nodes.

2.1 Security Requirements of Mobile Nodes

Basically, a mobile node (MN) roaming over the Internet SHOULD enjoy safe and persistent IP connectivity as much as this is permitted by the policies of its home and visiting subnets. Persistency of IP connectivity means that the connections should be handoff correctly and quickly so that the MN can maintain its TCP sessions when it changes its network attachment point. Safety means traffics to and from the MN should enjoy similar level of security (with respect to passive and active attacks) as it is on its home subnet.

The strong authentication of registration messages in both basic and route optimized Mobile IP is a crucial step to ensure correct and persistent IP connectivity for the MN. Nevertheless, this service must be augmented by the other security services (listed below in their priorities) as permitted or required by the security policies of the home and visiting subnets.

Notational remarks: In the specification of security services, following terms carry special meanings as described below:

authentication =	data origin authentication combined with connectionless message integrity - a typical IPSec service
optional =	security services to be employed only if it is explicit required by security policy.

2.1.1 Connectivity Protection between Mobile Nodes and Home Subnets

A MN SHOULD be allowed to have the same IP connectivity with the corresponding hosts (CHs) on its home subnet as it is on the home subnet. Security gateways guarding the home subnet MUST permit this level of connectivity once a policy consisting of some or all of the following security requirements is satisfied. The MN MUST be informed of any constraints to its home connectivity before or during Mobile IP registration.

- Authentication of traffic from the mobile node to its home subnet enforced by the security gateways protecting the home subnet (authentication of incoming traffic)

- [optional] Confidentiality of traffic between the mobile node and the security gateways protecting its home subnet

- [optional] Confidentiality of traffic between the mobile node and the corresponding hosts (end-to-end fine-grain protection)

- [optional] Authentication of traffic between the mobile node and the corresponding hosts (end-to-end fine-grain protection)

2.1.2 Connectivity Protection between Mobile Nodes and Other Subnets

The MN visiting the subnet SHOULD be allowed to communicate with a selected set of corresponding hosts (CHs) that is specified by the security policy of the visiting subnet. The permission of MN connectivity MUST be qualified by satisfaction of some or all of the following security services:

- [optional] Authentication of traffic from the mobile node to the security gateways protecting the visiting subnet (authentication of outgoing traffic)

  Note: reverse tunneling must be used if INGRES source filtering is employed by the security gateways.

- [optional] Confidentiality of traffic between the mobile node and the corresponding hosts (end-to-end fine-grain protection)

- [optional] Authentication of traffic between the mobile node and the corresponding hosts (end-to-end fine-grain protection)

The set of connectable CHs MAY be further limited by the security policy of MN's home subnet. This indirect application of security policy is beyond the scope of this document.

2.2 Security Requirements of Visiting Subnets

A foreign subnet visited by mobile nodes (MNs) SHOULD employ necessary measures (1) to restrict the use of its network resources (communication media, printers and servers) by the MNs and (2) to protect the traffic flows among local nodes from possible passive/active attacks launched by the MNs.

2.2.1 Protection of Network Resources

The access of the foreign subnet SHOULD be controlled when the MNs register through one of its foreign agents (FAs), and the access of selected resources (such as servers) MAY be further controlled by applying strong authentication and rule/identity-based access control to individual MN.

- Access control of the mobile node to the visiting subnet - if possible, the FAs SHOULD verify the identity of visiting MNs either directly or indirectly via their home agents (HAs) before issuing a care-of address to MN and permitting a successful completion of the registration process.

- [optional] Authentication of traffic between the mobile node and the corresponding hosts on the visiting subnet (end-to-end authentication)

2.2.2 Protection of Local Traffic

If the foreign subnet uses a shared medium such as Ethernet for communication then a visiting MN may eavesdrop, delete, insert or alter packets passing among the local hosts over the medium. Hence, encryption and message integrity checks SHOULD be in place to protect sensitive communication among the local hosts as well as between the local hosts and other MNs.

- [optional] Confidentiality and data integrity of traffic between local hosts on the visiting subnet

3. Use of IPSec on Mobile IP Redirection Tunnels

3.1 Operation Principles

This Internet Draft proposes a scheme of using IPSec ESP [ipsec-esp] protocol to protect selected Mobile IP redirection tunnels. These IPSec protected Mobile IP tunnels (MIP_IPSec tunnels) offer message confidentiality and authentication (including data origin authentication and connectionless integrity) but NOT anti-replay services to the IP datagrams to and from the mobile nodes (MNs) passing through the mobility agents, i.e. home agents (HAs) and foreign agents (FAs). We believe that selective use of these tunnels coupled with rule/identity based access control can provide the security services described in Sect.2.

The proposed scheme made certain assumptions on the architecture and implementation of this secure Mobile IP system. These assumptions are stated below:

- o In order to use the MIP-IPSec tunnels and the mobility agents for the best protection of the mobile Internet, both FAs and HAs SHOULD function as IPSec supporting security gateways capable of performing packet encryption/decryption and packet filtering based on strong authentication.

- o On a firewall protected foreign subnet, the FAs SHOULD be the firewalls closest to the mobile nodes (MNs). Other firewalls on the subnet SHOULD permit the IPSec protected packets to and from the FAs to pass through. Reverse tunneling must be used if INGRES source filtering is employed by the firewalls.

- o The HAs SHOULD function as the innermost firewall guarding the home subnet. Similarly, other firewalls on the subnet SHOULD permit the IPSec protected packets to and from the HAs to pass through.

- o The IPSec implementation is expected to be integrated with the Mobile IP implementation. Such an approach allows the use of a single IP-IP encapsulation to be used for both IPSec protection and Mobile IP packet redirection (except when MN-HA IPSec tunnels are used). The approach is also consistent with the new roles of FAs and HAs as IPSec supporting security gateways. Both the "bump-in-the-stack" (BITS) or the "bump-in-the-stack" (BITW) approaches will introduce an extra IP encapsulation.

3.2 Choice of IPSec Protected Mobile IP Tunnels

Figure 1 tabulates all the possible IPSec Mobile IP tunnels existing due to different Mobile IP options: collocated car-of-addresses [rfc200], reverse tunneling [mip-reverse-tunnel] and route-optimized Mobile IP [mip-optim]. The rows of the table list the tunnels roughly according to their importance in fulfilling the security requirement mentioned in Sect.2. The columns represent different combination of Mobile IP options, and the blank entries in the table imply the absence of the tunnels underneath specific Mobile IP options. Following notations are used in the table:

C,~C - denote the use and not use of collocated care-of-address.
R,~R - denote the use and not use of reverse tunneling.
T* - denotes the cases that an additional IPSec tunnel will be encapsulated within the Mobile IP tunnels.
Te - denotes the case that requires the use of encapsulated delivery from MN and FA in the implementation of Mobile IP reverse tunnels.
(T)- denotes the cases that duplicate the security functions of other

tunneling cases.
X - denotes the cases that correspond to IPSec protection between end hosts, and thus can be implemented using transport mode.
O - denotes the cases that exist only in route-optimized Mobile IP.

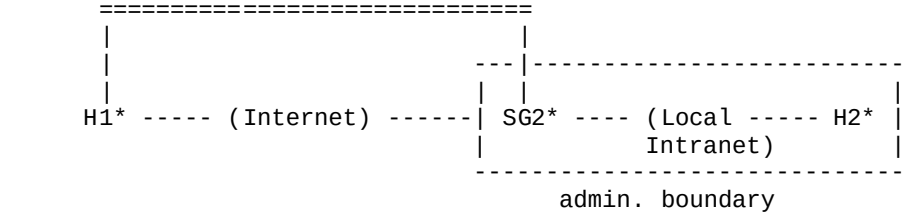
	~C,~R	C,~R	~C,R	C,R
HA -> MN	T*	T*	T*	T*
MN -> HA	T*	T*	T*	T*
HA -> FA	T	(T)	T	(T)
FA -> HA			T	(T)
FA -> MN	T		T	
MN -> FA			Te	
CH -> MN	X	X	X	X
MN -> CH	X	X	X	X
CH -> FA	O	O	O	O
FA -> CH	O	O	O	O
CH -> HA				
HA -> CH				

Figure 1. Choices of IPSec Protected Mobile IP Tunnels

The MIP-IPSec tunnels running between MN-HA, HA-FA, FA-MN are the essential ones for fulfilling the security requirements. They will be examined individually in the following paragraphs. In addition, the end-to-end IPSec protection between MNs and CHs can be used in combination with the IPSec tunnels. Notice that Mobile IP tunnels do NOT run between CHs and HAs, and the tunnels running between CHs and FAs exist only in route-optimized Mobile IP. This is because corresponding hosts may be completely ignorant of Mobile IP, and may not know of the existence of FAs and HAs.

3.2.1 MN-HA Tunnels

The MN-HA MIP-IPSec tunnels can be used to provide data-origin authentication plus connectionless integrity and data confidentiality. They are most useful in providing a secure communication path between a MN and its home subnet as described in [ipsec-arch, case 4] as shown in the following diagram.



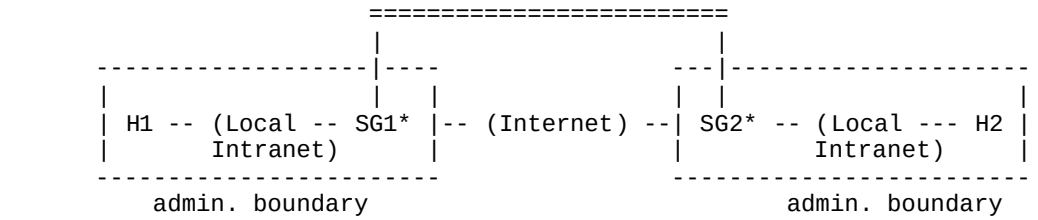
The data-origin authentication and connectionless integrity can counter active attack while data confidentiality can frustrate eavesdropping. By using the tunnels in both directions, a MN SHOULD be allowed to enjoy same connectivity as it has at home.

The MN-HA tunnels are, however, more expensive to establish -- since they are NOT one of the Mobile IP redirection tunnels, they must be established separate- ly with the use of an additional IP header.

3.2.2 HA-FA Tunnels

The MIP-IPSec tunnel going from a HA to a FA (and from a FA to a HA if reverse tunnel and FA Care-of Address are used) can be implemented by simply adding IPSec protection to the existing Mobile IP tunnels.

The tunnels can also be used to support data-origin authentication plus connectionless integrity and data confidentiality. They establish virtual private network (VPN) connections between the home subnet of the MN and the foreign subnet currently visited by the MN as shown in the following diagram.



The main uses of the FA-HA tunnels are (1) to frustrate passive and active attacks from the open Internet, and (2) to traverse firewalls between FAs and HAs. Such a tunnel MAY allow the MN to access its home subnet only if it is coupled with strong authentication of the MN by the FA and system security of the FA.

3.2.3 MN-FA Tunnels

The MN-FA MIP-IPSec tunnels can be used in two ways if no link-layer protection has already provided the services:

1. data confidentiality for MN over the foreign network and
2. data origin authentication of MN-FA exchange.

The MN-FA tunnels exist only if MN chooses to use an FA Care-of Address and they must be built by re-encapsulating the IP datagrams. Hence, these tunnels are ex- pensive to use and should be replaced by MN-CH end-to-end IPSec protection or MN-HA IPSec tunnels whenever possible.

4. Changes to Mobile IP Messages

In order for the mobile nodes (MNs) and the mobility agents (FAs and HAs) to agree on the selection of MIP-IPSec tunnels, the FA and the MN SHOULD use the following two extensions (added to the mobility agent advertisement and the registration request) for proposing their choices. Upon reception of the registration request, the HA SHOULD decide weather to accept and reject the proposal based on its security policy and then return its decision using the return codes in the registration reply. Such a selection process is deemed necessary owing to the difficulty of formulating static IPSec policies to handle the migration of mobile nodes. Because FAs and HAs SHOULD only serve the MNs if they complete the registration process, it is necessary to devise a mechanism to generate the IPSec policies for the selected tunnels and insert them into the security policy database (SPD) at the end of the process.

4.1 Extension to Mobility Agent Advertisement

An FA IPSec Tunnel Extension is added to the mobility agent advertisement message, which conforms to the format of an ICMP router advertisement. The purpose of the extension is to carry FA's choice of MIP-IPSec tunnels. The type- length-value (TLV) format of the extension is shown in Figure 2.

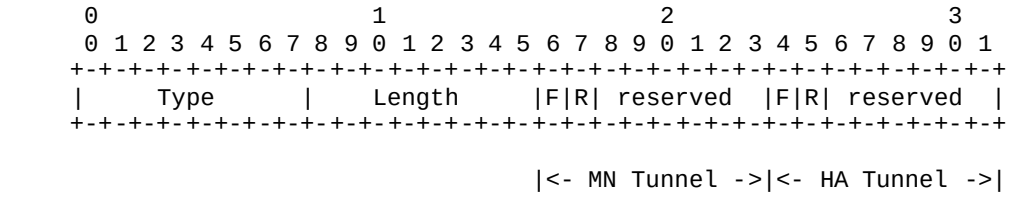


Figure 2. FA IPSec Tunnel Extension

Type [TBD]

Length 2 bytes

F IPSec Protection for Forward Tunnels (HA->FA, FA->MN)

R IPSec Protection for Reverse Tunnels (FA->HA, MN->FA)

reserved IGNORED upon reception; MUST be set to ZERO during transmission

4.2 Extension to Mobile IP Registration Request

An MN IPSec Tunnel Extension is added to the registration request message. This extension indicates the choices of MIP-IPSec tunnels made by MN based on its own policy and its knowledge of FA's choices. The extension carries SIX flags, each when SET indicates the use of IPSec on a possible tunnel. The extension format is shown in Figure 3. To simplify processing, the flags in the FA IPSec Tunnel Extensions remain in the same positions.

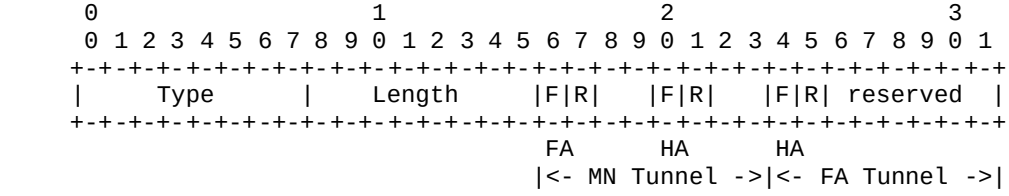


Figure 3. MN IPSec Tunnel Extension

Type [TBD]

Length 2 bytes

F IPSec Protection for Forward Tunnels (HA->FA, FA->MN, HA->MN)

R IPSec Protection for Reverse Tunnels
(FA->HA, MN->FA, MN->HA)

reserved IGNORED upon reception; MUST be set to ZERO
during transmission

4.3 Mobile IP Registration Reply

FOUR error codes are added to the registration reply for conveying possible failures of the tunnel selection process.

Service denial by HA:

Values	Semantics
[TBD]	Tunnel Selection Conflict
[TBD]	Tunnel Selection Unsupported

Service denial by FA:

Values	Semantics
[TBD]	Tunnel Selection Conflict
[TBD]	Tunnel Selection Unsupported

5. Procedure for MIP-IPSec Tunnel Establishment

The process of establishing the MIP-IPSec tunnels can be divided in three steps: (1) tunnel selection, (2) security association negotiation and (3) tunnel activation. Among them, tunnel selection happens concurrently with Mobile IP registration and tunnel activation occurs also in ordinary Mobile IP tunneling. The insertion of security association (SA) negotiation is a new step, and it introduces a new complexity to the process: owing to the possible failure of SA negotiation, a MIP-IPSec tunnel MAY need to be dismantled even after a success- ful Mobile IP registration. The case will be discussed in a following section.

5.1 Selection of MIP-IPSec Tunnels

Like Mobile IP registration, the tunnel selection process begins with mobility agent advertisement. FAs SHOULD announce their IPSec tunneling requirements in the FA IPSec tunnel extension after consulting their security policies. The advertisement is usually NOT authenticated due to the lack of key management prior to this process.

After receiving the advertisement message, an MN MAY response by

sending an MN registration request to the FA, and MAY attach an MN IPSec tunnel extension to the request. The extension MUST carry the choice of MIP-IPSec tunnels made by the MN based on its own security policy and FA's choice conveyed in the advertisement. The registration request including the extension MUST be authenticated to the HA of the MN, and MAY also be authenticated to the FA if keys have been exchanged between the MN and the FA.

Upon receiving the registration request, FA MUST compare its own choices of IPSec tunnel with the corresponding choices of the MN, and return a "Tunnel Selection Conflict" error in an FA registration reply to MN if a mismatch is found. Otherwise, FA SHOULD forward the registration request to the HA.

When the HA receives the registration request, it MUST check the IPSec tunnel choices against its own security policies (beside of making other Mobile IP registration decisions). HA MUST return a "Tunnel Selection Unsupported" error in an HA registration reply if the choices are incompatible to its policies.

Any error code in the registration replies MUST cause the failure of the registration process. A successful registration process will cause appropriate entries to be inserted in the IPSec SPD in MN, FA and HA as a preparation for subsequent SA negotiations.

5.2 Negotiation of Security Associations and Keys

The negotiation process is analogous to that of an ordinary IPSec tunnel esta- blishment. A successful Mobile IP registration promises only IP connectivity between the mobile node and the relevant mobility agents, but leaves the IP traffic without any protection. SA negotiations SHOULD then be conducted through these unprotected IP tunnels using protocols like ISAKMP [isakmp]. A failure of the negotiations SHOULD imply a failure of establishing the corresponding MIP- IPSec tunnel. Thus, it MUST cause the generation of proper error events and the prohibition of any secure communication via the corresponding tunnel. Whether the Mobile IP tunnel should be dismantled SHOULD be decided according to the Mobile IP policies enforced by the end points.

5.3 Activation of MIP-IPSec Tunnels

Since the existence of Mobile IP tunnels do NOT necessarily imply the existence of corresponding MIP-IPSec tunnels, the IPSec tunneling services MUST only be activated after the successful negotiation of necessary security associations. Before such activation, only limited types of traffic, e.g. key management exchanges, are allowed to use these tunnels. General traffic can only use the tunnels when

the required IPSec services are in place.

6. Format of Encapsulated Packets

In the cases that IPSec tunneling services are added to the existing Mobile IP tunnels, both tunnels SHOULD be implemented using a common IP-IP encapsulation [Sect.6.1]. In the only case of MN-HA tunneling, an MN-HA IPSec tunnel MUST be embedded into outer Mobile IP (HA-FA, FA-MN) tunnels. Hence, an extra IP header will be inserted along with ESP header between the Mobile IP encapsulation and the original IP header.

The IP encapsulation can be implemented using either full IP-IP encapsulation [full-ipip] or minimal IP-IP encapsulation [mini-ipip]. The only exception is that the extra IP header that implements the MN-HA IPSec tunnel can NOT be in the form of minimal encapsulation.

7. References

[rfc2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Level," RFC-2119, March 1997.

[rfc2002] C. Perkins (ed.) "IP Mobility Support." RFC2002, proposed standard. IETF Mobile IP Working Group, Oct. 96.

[mip-optim]D.B. Johnson, C. Perkins. "Route Optimization in MIP." <draft-ietf-mobileip-optim-03>, IETF Mobile IP Working Group, Nov. 95.

[mip-tunnel-reverse]G. Montenegro. "Reverse tunneling for Mobile IP". <draft-ietf-mobileip-tunnel-reverse-02>, IETF Mobile IP Working Group, Mar. 97.

[isakmp] D. Maughan, M. Schertler, M. Schneider, J. Turner. "Internet Security Association & Key Management Protocol (ISAKMP)" <draft-ietf-ipsec-isakmp-07>, IPSec Working Group, Feb. 97.

[ipsec-arch]S. Kent, R. Atkinson. "Security Architecture for the Internet Protocol." <draft-ietf-ipsec-ipsec-arch-??>, IETF Network Working Group, Aug. 95.

[moips] J. Zao, S. Kent, J. Gahm, G. Troxel, M. Condell, P. Helinek, N. Yuan, I. Castineyra. "A Public-Key Based Secure Mobile IP". MobiCom97. Sep. 97.

Disclaimer

The views and specification here are those of the authors and are not necessarily those of their employers. The authors and their employers specifically disclaim responsibility for any problems arising from correct or incorrect implementation or use of this specification.

Author Information

Dr. John K. Zao
BBN Technologies
70 Fawcett Street
Cambridge, MA 02138
USA
E-mail: jzao@bbn.com
Telephone: +1 (617) 873-2438

Matt Condell
BBN Technologies
10 Moulton Street
Cambridge, MA 02138
USA
E-mail: mcondell@bbn.com
Telephone: +1 (617) 873-6203