IP Routing for Wireless/Mobile Hosts (mobileip) WG
INTERNET-DRAFT
Date: 05 November 2001
Expires: May 2001

Allison Mankin
Basavaraj Patil
Dan Harkins
Erik Nordmark
Pekka Nikander
Phil Roberts
Thomas Narten

Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6

<draft-ietf-mobileip-mipv6-scrty-reqts-02.txt>

Status of This Memo

Abstract

The IESG returned the Mobile IPv6 (MIPv6) draft to the working group due to concerns about the security and scalability of binding updates (BUs) sent to correspondent nodes and the associated IPsec processing that is specified in the draft. Since that time discussions have continued to attempt to define what is really needed to make binding updates secure while taking into consideration the aspect of scalability as well as the fact that IPsec may not be the most suitable security mechanism for securing BUs between MNs and CNs. In

the course of discussing the requirements it became apparent that a threat model is needed in order to adequately specify the security requirements. Mobile IPv6 mandates that all binding updates be authenticated. The current approach taken to securing these BUs is via the use of IPsec. This approach for securing BUs has various problems, one of which is scalability. The I-D from a specification perspective does not have security vulnerabilities, but as specified, has serious limitations in its capability to be deployed on an Internet wide basis.

The purpose of this I-D is to identify the scenarios and threats that Mobile IPv6 can possibly bring to the Internet. From these scenarios and threats are derived a set of requirements that Mobile IPv6 needs to address as part of the specification.

Table of Contents

1. Introduction

The IESG returned the MIPv6 draft to the working group due to concerns about the security and scalability of binding updates (BUs) sent to correspondent nodes and the associated IPsec processing that is specified in the draft. Since that time discussions have continued to attempt to define what is really needed to make binding updates secure while taking into consideration the aspect of scalability as well as the fact that IPsec may not be the most suitable security mechanism for securing BUs between MNs and CNs. In

the course of discussing the requirements it became apparent that a threat model is needed in order to adequately specify the security requirements.

The purpose of this I-D is to identify the scenarios and threats that Mobile IPv6 can possibly bring to the Internet. From these scenarios and threats are derived a set of requirements that Mobile IPv6 needs to address as part of the specification.

The goal is to determine which of those threats are of concern and should be defended against. While the basic goal is "no worse than IPv4," the prevalence of wireless and the likely deployment of MIPv6 in that space means the basic goal should aim at being "no worse than IPv4 with switched Ethernets", although the intent is not to try to solve the security problems of shared/broadcast wireless mediums. The threat model is used to generate a list of requirements to make the MIPv6 protocol secure against likely threats. These requirements, interspersed with the threats and also listed at the end of this document are aimed at providing guidelines in developing a solution for MIPv6 security.

For the readers that are new to computer and communications security, we recommend consulting Appendix A, "Background", for some introductory material.

1.1. Assumptions

The Mobile IPv6 specifies that basically any IPv6 node MAY function as a Correspondent Node (CN), receiving Binding Updates and creating Binding Cache Entries. However, any node MAY alternatively ignore, either selectively or altogether, Binding Updates, and continue sending packets to the Home Address. Additionally, a Corresponding Node may itself be a Mobile Node. It should be noted that most threats if not all arise from the BU that is sent by the MN to the CN, and that too only when the CN processes the BU itself, thereby creating a binding cache or, when it processes the home address option in an IPv6 packet without authorization to do so.

Furthermore, the following assumptions are made in the threat analysis below:

1 The mobile node and the HA have setup a pre-established bidirectional security association before the mobile node begins to roam and connects to the network from a location that is not its home. This does not imply that the MN has to always boot up at home before roaming onto other networks. The reason for a bidirectional SA is to authenticate the BU as well as the BAck.

The nature of this security association is not elaborated in this document. But it is anticipated that it is quite feasible to assign keys or certificates between a MN and an HA. This assumption is due to the likelihood that an MN and Home Agent belong to the same administrative domain, or else are in a business relationship of some sort. The unusual cases in which this is not true ("homeless" MN) will have additional security issues, which will need to be separately considered in the future.

This security association may be established by configuring the keys or certificates etc. on the MN and the home network at the time of subscription.

2 In most cases there are no existing, established security associations or other security relationships between the mobile node and the correspondent node. In addition no Certificate authorities nor a PKI exist that would enable the establishment of such SAs dynamically. The reason for requiring a SA between the MN and a CN is because the BU sent by the MN to the CN needs to be secured in order to avoid possible threats identified in this I-D.

2. Terminology/Definitions

1 Passive Attacks In a passive attack, the attacker reads packets off the network but does not write them. Eg: For instance, password sniffing attacks can be mounted by an attacker who can only read arbitrary packets. This is generally referred to as a PASSIVE ATTACK.

2 Active Attacks When an attack involves writing data to the network, we refer to this as an ACTIVE ATTACK.

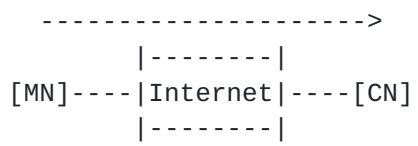
3. Threats on a broad scope introduced by Mobile IPv6

An intrinsic feature of any mobility scheme is, obviously, mobility. Thus, node mobility accomplished via Mobile IPv6 raises a number of security issues. The most damaging threat that MIPv6 introduces is the ability to redirect packets from communicating IPv6 peers. A redirect attack can be defined as an attack in which mobility signaling causes the route that packets take between two communicating peers to be altered such that the packets are routed to a destination determined by the attacker. The ability to redirect packets can allow an attacker to insert himself in the middle of a session (MITM) quite easily. Redirect attacks can also be launched from remote locations and attackers do not have to be on the same link as the communicating peers.

Other mobility introduced threats are denial-of-service (DoS) threats, basically meaning that a hostile node may be able to block all traffic on an unprotected link, or a dishonest (wireless) link operator may cause DoS or other harm to a mobile node.

Another class of threats is created by the Mobile IPv6 route optimization mechanism. A Mobile Node (MN) has the capability to send a Binding Update to a Correspondent Node (CN) in order to achieve route optimization of the packet stream from the CN to the MN. Normal packet routing without Binding Updates sent to CNs works as follows:

Packet stream from MN to CN:

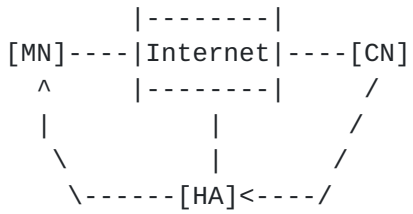


SRC Addr: MNs CoA

Dst Addr: CNs Global IPv6 address

Dest opt: MNs Home Address in Home Address option

Packet stream from CN to MN:



CN to HA:

SRC Addr: CNs Address

Dst Addr: MNs Global IPv6 home address

HA to MN:

Tunnelled

A Binding Update can be sent by the MN to a CN, which results in a Binding Cache Entry for the MN being created in the CN (See Section 8.3 of [1]). However it should be noted that a CN will create the entry in the Binding Cache iff the rules specified in Sec 8.2 of [1] are satisfied. Subsequent packets from the CN to the MN will include a routing header which contains the MNs home address and the destination address in the IP header is the MNs CoA (thereby achieving route optimization and bypassing the HA from the packet stream).

4. Classification of Threats

In the absence of a security association between most MN-CN pairs, there are multiple vulnerabilities that the MN, the CN, or the HA or home network, become exposed to. Basically, the threats can be classified as follows.

1 Tampering with the Binding Cache Entries

- creating an unauthorized Binding Cache Entry at a Home Agent

(Note that this threat is mostly covered by the assumption of having a security association between the MN and the HA. However, we do include some discussion in order to clarify some of the authorization and security policy issues involved.)

- creating an unauthorized Binding Cache Entry at a Correspondent Node

- creating an unauthorized Binding Cache Entry at the previous access router, acting as a temporary packet forwarding Home Agent

2 Denial-of-Service

- preventing a MN from communicating with some or all nodes

- preventing a CN from communicating with some or all nodes

- preventing a HA from serving legitimite MNs

3 Disclosure of sensitive information

- Disclosure of nodes serving as home agents in a network

5. Classification of Attackers

The following classes of attackers, and threats caused by them, are considered:

- an arbitrary node, anywhere in the Internet, launching an attack gainst a MN, a CN, or a HA

- an attacker located on the same (wireless) link as the MN

- an attacker located on the same link as the CN

- an attacker located on the same link as the HA

- an attacker on the path between the CN and the HA

- an attacker on the path between the MN and the CN

Please note that we do not consider the case where an attacker is on the path between the MN and HA, since we assume that their communication is secured or can be secured via the existence of the MN-HA security association. Note, however that the current Mobile IPv6 specification (version -14 of [1]) makes no assumptions about the MN-HA path traffic being secured.

Furthermore, we consider the following threats separately:

- using a previous router as a temporary HA
- DoS attacks against a CN
- DoS attacks against a MN
- DoS attacks against a HA

6. Detailed threat scenarios

In this section, we present a number of specific threat scenarios. The scenarios are arranged by the capabilities of an attacker, using the same order as the classification above. Some of the threats are specific to Mobile IPv6 while other's are not. The inclusion of the non-related threats serves as a background to evaluate the related threats.

To make cross referencing easier, the scenarios can be classified as follows:

	Attack	Attacker location	Effect	Remarks
A.	1	Anywhere	MITM/DoS	Needs to know Home Address
	2	Anywhere	MITM/DoS	Needs to know Home Address
	3	Anywhere	DoS	No prior knowledge needed
B.	1	MN's link	MITM/DoS	Using only BUs
	2	MN's link	MITM/DoS	Using non-MIPv6 mechanisms
	3	Close to MN	MITM/DoS	Tamper with radio interface
	4	MN's link	MITM/DoS	Tampering Binding Acks
C.	1	CN's link	MITM/DoS	Using non-MIPv6 mechanisms
D.	1	HA's link	MITM/DoS	
	2	HA's link	Multiple	Acting as a Home Agent
E.	1	CN->HA link	Masq/DoS	Attack without BUs
	2	CN->HA link	MITM/DoS	Defeat Home Address check
F.	1	MN->CN link	DoS	Attack without BUs
	2	MN->CN link	MITM/DoS	Immune to ingress filtering
G.	1	MN's (past) link	MITM/DoS	Fool temporary HA
H.	1	Anywhere	Disclosure	Topology information exposed

2	Anywhere	DDoS	Use HA as a reflector
3	Anywhere	DDoS	Use CN as a reflector

6.1. Threats related to attackers located anywhere in the internet

6.1.1. Tampering with the CN binding cache

The following section describes scenarios, threats, effects and requirements that deal with manipulating the binding cache in the CN.

6.1.1.1. Scenario 1 - Attacker knows MNs home adress

A MN and a CN have an ongoing session. A malicious node/attacker knows the MNs home address.

6.1.1.1_Threat:

The attacker can send a binding update to the CN. The CN believes that the MN has moved and hence has a new CoA. It updates the entry for the MN in its binding cache.

6.1.1.1_Effect:

The packet stream for the ongoing session from the CN to the MN now is diverted to the malicious node.

The MN in this case may be on its home network and not have any CoA or it may be on another network and have a CoA. The attacker in this case only needs to know about the MNs home address and possibly any CNs that the user may communicate with. The attacker could be anywhere on the Internet and does not have to be on the same link or network as the MN.

6.1.1.1_Reaction:

In the above case the MN may realize that it is no longer receiving any further packets from the CN and may take appropriate actions, which may include sending another binding update to the CN.

The attacker has the ability to redirect the traffic to another location via this attack. If not for any gains, this kind of an attack can be classified as a DoS attack. Such an intruder could also send a BU to the MN supposedly from the CN and insert himself as a MITM for traffic between the two.

The attack described here is an active binding cache update attack. The CNs binding cache has been changed by an entity that does not own the home address sent in the BU. So the issue is, how does a CN determine if the sender of the BU actually is authorized to create cache entries for the home address carried in the BU, before updating his binding cache.

A DoS attack or MITM attack on an IPv6 node can be mounted even if the node never goes mobile. Since it is possible to create an entry in the binding cache for an IPv6 node in another IPv6 node, it is not required that a node be mobile or have mobile IP client software on it to be able to do it. In the absence of verifiability of the authority over the IPv6 home address of a node, another IPv6 node can send a BU to any other IPv6 node on behalf of someone else and cause disruptions in communications between legitimate IPv6 nodes.

6.1.1.1_Requirement:

A correspondent node MUST not update its binding cache on receiving a binding update from any IPv6 node without verifying that the packet was sent by a node authorized to create binding cache entries for the home address carried in the home address option of the BU.

6.1.1.2. Scenario 2 - ICMP unreachable sent to CN

An ICMP unreachable message can be originated as a result of packets from the CN not being able to be delivered to the MN at it's COA (or its Home Address). The ICMP unreachable message would normally be sent by the last hop router serving a MN if the MN has moved and is no longer attached to the network via that router.

6.1.1.2_Threat:

An attacker could send an ICMP unreachable for an MNs COA to a CN which has created a binding cache entry for that MN.

6.1.1.2_Effect:

The CN deletes the binding cache entry for that MN. The result is that the traffic stream from the CN to the MN are now routed through the HA. Route optimization fails, but the traffic stream between the MN and CN is still maintained.

6.1.1.2_Requirement:

No Mobile IPv6 specific requirements can be generated from this threat.

6.1.2. Tampering with the MNs binding cache

In the previous section we looked at changing the binding cache entry for an IPv6 MN in the CN. However an MN can also be considered as a CN from the perspective of being an end-point in a session that is being terminated at the MN and originated from another MN. In such a case the MN (now in the role of a CN) also has a binding cache entry for the other MN. The same threats discussed above are now opened up on the MN.

6.1.2.1. Scenario 3 - Both end-points of a session as MNs

If a MN originates a VoIP call to a CN which is also mobile, the MN sends the CN a binding update to achieve route optimization. The CN will also in this case send a BU to the MN (originator) and update the binding cache. An attacker could possibly determine the end-points of this session by various means. For example, it may learn about the call/session by eavesdropping on the local link of either party, or possibly by eavesdropping on the SIP signalling elsewhere in the internet.

6.1.2.1_Threat:

An attacker can send a BU to either the MN or the CN or both and disrupt the communication. So, a passive attacker could be just sitting and learning about the VoIP call, and possibly launch the malicious BU to the MN and the CN from another network.

6.1.2.1_Effect:

Cause packets to be routed to the incorrect destination, leading to either denial-of-service or snooping (privacy violation) or worse modifying the content of the traffic by MITM.

6.1.2.1_Requirement:

Same as Req 6.1.1.1_Requirement

<Comment1 in Appendix B>

6.1.3. BU flooding

This section deals with threats that are related to nodes involved in mobility being flooded by BUs.

6.1.3.1. Scenario 4 - BU flooding

Malicious nodes could flood a CN with fake BUs affecting the binding cache.

6.1.3.1_Threat:

A malicious node or virus could keep sending fake BUs to other IPv6 nodes at a very rapid rate and thereby create unnecessary state in an IPv6 node. It could also possibly cause the binding cache memory to become inundated with entries for nodes that have no real meaning and thereby preventing a valid node's entry being created in the binding cache.

6.1.3.1_Requirement:

a) An IPv6 node that receives binding updates SHOULD NOT create state until it has verified the authenticity of the sender.

b) An IPv6 node SHOULD have the capability to reject binding updates.

6.2. Threats related to attacks originating from the same subnet/link as the MN

There are multiple possibilities here depending on the type of access medium. If the access medium is a shared multiple access network such as a wireless network (802.11, wide-area cellular) or an Ethernet LAN, the attacker could do passive monitoring of the packets. The attacker could possibly not intercept the packets and forward them unless he takes on the role of the default router and cause packets from the MN to be delivered to him instead of the actual default router. However this threat can be classified as a general threat and one that is not specific to Mobile IPv6.

6.2.1. Scenario 5 - MITM via a spoofed BU

A man-in-the-middle attack can be mounted on an ongoing session by sending a spoofed to the CN or the MN.

6.2.1_Threat:

By being able to passively monitor the traffic, the attacker could learn about the CNs that the MN is communicating with and also determine to which CNs the MN is sending BUs. The attacker could in such a case send a spoofed BU packet to the same CN. Furthermore, it can very easily send a spoofed BU to the MN, claiming that the CN is currently on the same link as the MN (i.e. co-located with the attacker).

6.2.1_Effect:

This will cause the traffic from the CN to the MN be routed elsewhere. Changing the route of packets from CN to MN is a serious threat. It can be classified as a DoS attack on the MN or the CN. The latter case where the attacker also sends a BU to the MN results in a MITM, where the attacker could possibly alter the contents of the traffic.

6.2.1_Requirement:

Same as verifying if the sender is authorized to send BUs for the home address contained in the BU.

6.2.2. Scenario 6 - Man-in-the-middle attack via the default router

A man-in-the-middle attack could be launched on hosts attached to a link by having them change their default router

6.2.2_Threat:

If the attacker takes on a more active role, it can insert itself as a MITM between the MN and the CN, by pretending to be the default router to the MN and the MN to the CN.

6.2.2_Effect:

The attacker could possibly modify/change the contents of the traffic. On a wired or wireless LAN or wireless network, the attacker cannot prevent the router advertisements from the default router (DR) reaching the MN. So it would probably be difficult for the attacker to intercept packets to/from the MN by pretending to be the DR. However the attacker who is on the link and monitoring the router advertisements can in effect send a new router advt. (proclaiming himself as the DR) immediately after the actual routers advt and thereby overriding the true routers advt. from the MNs perspective. If an attacker can take on the role of the default router there are other more significant threats than the ones that Mobile IP introduces and it goes for both v4 and v6.

6.2.2_Requirement:

This is not specific to Mobile IPv6 and hence no requirement is generated as a result.

6.2.3. Scenario 7 - Moving to an untrusted access point

The MN could attach itself to an access point that has not been authenticated.

6.2.3_Threat:

The attacker could easily have a WLAN access point and cause the MN to switch to the new AP and a different network (maybe) on which the attacker could be at the DR and thereby able to intercept and modify packets on the uplink and downlink.

In this attack, the attacker uses the original base station as its uplink, and pretends to be a single node to the original base station.

6.2.3_Effect:

In this type of an active attack, the MN continues its session with the CN, but in the case where the attacker uses the original base station the binding cache entry for the MN in the CN is that of the attacker's address. The attacker continues to forward doctored packets (received from the CN) to the MN. The attacker essentially changes the destination address from it's own (CoA) address to the MNs CoA before forwarding the packets and the MN as such is unaware of the MITM.

The CN is unaware that the packets to the MN are now being sent to another node as there is no way that the CN could verify the ownership of the home address in the BU.

In the case of a wide area wireless network (CDMA/TDMA) it is possible to mount a passive attack on the traffic between the MN and the CN on the air-interface. However it would be much more difficult (cost-perspective) in having a MN change the AP/BTS that it is currently using. The attacker can learn the details of the MN and it's communicating partners and mount an attack from elsewhere.

The CN which continues to receive packets from the MN (with src address, MNs CoA) has also received a BU from the attacker and has changed the entry for the MN in it's binding cache. As a result the CN's packet stream to the MN will flow to the attacker at the address

specified. The CN may tend to believe that the CoA sent in the BU is an alternative CoA which MIPv6 allows.

6.2.3_Requirement:

The Mobile Node SHOULD be capable of ascertaining the identity of the access point to which it is attaching and authenticate it.

6.2.4. Scenario 8 - Passive monitoring of traffic

An attacker who is able to passively monitor the traffic could send a fake Binding Ack to the MN as a response to a BU sent by the MN.

6.2.4_Threat:

By being able to passively monitor the traffic, the attacker could learn about the CNs or HA that the MN is communicating with and also determine to which CNs or HA the MN is sending BUs. The attacker could thus synchronize with the MN such that when MN sends a BU then attacker replies to MN with a fake Binding Acknowledgment different than the true Binding Acknowledgment (Status, Lifetime or Refresh fields).

6.2.4_Effect:

This can lead to (1) MN sends unnecessary BU's (subject to rate limiting of sending BU's) or (2) MN doesn't send a BU that is necessary. As further effects of (2) unnecessary triangular routing takes place or MN is not reachable at all.

6.2.4_Requirement:

Upon receiving a packet carrying a Binding Acknowledgement, a mobile node SHOULD ensure it trusts the sender of that Binding Acknowledgment.

<Question1 in Appendix B>

6.3. Threats related to attacks originating from the same subnet/link as the CN

The fact that the attacker can be on the same link as the CN has other implications as well. When considering this possibility most of the same issues already outlined apply. In many cases the CN may also be an MN to a different CN and in that case all the attacks listed above apply here as well.

6.3_Threat:

It should be pointed out that in the absence of MIPv6 today an attacker on this link is able to accomplish quite a lot of mischief, such as spoofing neighbor discovery or inserting itself as an MITM using link level techniques.

It is also easier for the attacker to now insert himself as a MITM and intercept and modify packets sent between the MN and the CN. So an attacker on the CNs link can mount an active attack more effectively than if he is on the MNs link.

6.4. Attacker located on the same subnet/link as the HA

If a mobile node is on its home network, it does not need to send any binding updates to CNs and as such Mobile IP is not required.

6.4.1. Scenario 9 - Spoofed BUs sent on behalf of an MN which is at home

An attacker on the same subnet as the MN (on its home subnet) could send BUs to CNs that the node is communicating with and disrupt the traffic.

6.4.1_Threat:

An attacker on the same subnet as the MN (on its home subnet) could send BUs to CNs that the node is communicating with and disrupt the traffic. Since the attacker is on the same subnet as the MN, i.e. at home, it may be aware of the CNs that the MN is communicating with. Therefore it can easily send a BU to these CNs and inform them that the MN is now reachable at some COA.

6.4.1_Effect:

Traffic disruption by diverting the packets to an unwanted COA; DoS attack agains the MN, or Man-in-the-Middle attack with some more effort.

6.4.1_Requirement:

Same as verifying if the sender is authorized to send BUs for the home address contained in the BU.

With some more effort, the attacker can insert himself between the MN and the CN, even when the MN is at home. That is, the attacker sends a BU on the behalf of the CN to the MN, telling that the CN is a

mobile node and currently co-located at the same network as the MN is. Simultaneously, it sends a BU to the CN telling the CN that the MN is currently at the attacker's address. Since the CN is not assumed to check that the Home Address and the COA are at different subnets, there is no reason why the latter wouldn't work either.

6.4.2. Scenario 10 - Intercepting BUs sent to HA

If the attacker is on the same subnet as the HA of an MN, the attacker could possibly intercept the BU packet the MN sends to the HA (while the MN is roaming). The attacker could spoof the HA and send a Binding request to the MN even when it is not required.

6.4.2_Threat:

If the attacker is on the same subnet as the HA of an MN, the attacker could possibly intercept the BU packet the MN sends to the HA (while the MN is roaming). The attacker could spoof the HA and send a Binding request to the MN even when it is not required. Binding requests can also be sent by other malicious nodes to the MN or in the worst case scenario, the MN could be flooded by binding requests from an attacker with spoofed source IP addresses.

6.4.2_Effect:

1 DoS for the MN as the Binding update could be rejected.

2 The attacker himself pretends to be the HA and begins to intercept traffic destined for the MN originating from the CNs.

3 The MN may not be sending BUs to CNs in order to maintain location confidentiality. However Since the attacker is aware of the COA of the MN at all times, the location privacy of the MN is lost.

4 Flood the MN with a large number of binding requests.

6.4.2_Requirement:

The MN SHOULD be capable of authenticating binding requests. The MN SHOULD/MAY only process binding requests which are originated by nodes that are in the binding update list of the MN.

6.4.3. Scenario 11 - BU cancellation at HA by malicious node

A malicious node on the home subnet can send a binding update to the HA for an MN with lifetime set to zero and thereby cause the binding cache entry to be deleted.

6.4.3_Threat:

A malicious node on the home subnet can send a binding update to the HA for an MN with lifetime set to zero and thereby cause the binding cache entry to be deleted. The malicious node could cause the HA to believe that the MN has returned to its home network and hence does not need a binding to some COA.

6.4.3_Requirement:

The HA MUST authenticate any binding update received by it before making any changes to the binding cache entries.

<Comment2 in Appendix B>

6.5. Attacker on the path between the CN and HA

If an attacker is able to insert himself on the path between the CN and the HA, it may open up the following security gaps.

6.5.1. Scenario 12 - Masquarade/DoS attack

6.5.1_Threat:

If the MN and CN are communicating via Mobile IPv6 but the MN is not sending Binding Updates to the CN, all packets originated by the CN are first sent to the Home Address. The packets are then received by the HA, and tunneled to the MN. Now, if the attacker is on the CN-HA link, including CN's local link and the HA link, it is able to eavesdrop on all traffic flowing from the CN to the MN. Thus, if the MN is not on-line, the attacker can easily play the MN's part, and masquerade as an MN. On the other hand, if the MN is on-line, the attacker can easily disrupt communications e.g. by sending TCP RSTs.

6.5.1_Effect:

Masquarade when the MN is off-line, DoS otherwise.

6.5.1_Requirement:

Any requirements to address this threat is outside the scope of Mobile IPv6 as the threat described above is a generic one. However MIPv6 itself SHOULD not cause further grief in establishing end-to-end security either using IPsec or other mechanisms.

6.5.2. Scenario 13 - CN challenge to a BU sent by the MN

6.5.2_Threat:

If the MN sends a binding update to the CN and the CN rather than updating the cache decides to challenge the MN to verify if in fact the MN was the one that originated the BU, it can send a challenge/cookie/foobar to the MNs home address instead of the CoA. If the routing infrastructure is intact, the home agent of the MN will receive this packet containing the challenge and will forward/tunnel the packet to the MN (maybe over a secure tunnel). The MN on receiving the challenge/cookie may act on it and send it back to the CN. The CN on receiving the challenge it sent out originally to the MNs home address has reason to believe that the MN was indeed the one that originated the BU and can go ahead and create an entry in the binding cache.

However if the attacker is on the CN-HA path, including CN's local link and the HA link, s/he can intercept this packet containing the challenge and send a spoofed response to the CN and cause it to create an invalid entry for the MN in it's binding cache. The attacker on the CN-HA path and an attacker on the MNs link could be co-conspirators and be able to insert themselves in the communication path.

6.5.2_Effect:

Ability to insert onself as a MITM.

6.5.2_Requirement:

Same as verifying if the sender is authorized to send BUs for the home address contained in the BU.

6.6. Attacker on the path between the MN and CN

If the MN is not at home, and the attacker is on the path between the MN and the CN (including the MN's and CN's local link), it can eavesdrop on packets sent by the MN to the CN. Therefore it can easily learn the Home Address of the MN.

6.6.1. Scenario 14 - Non MIPv6 Specific

6.6.1_Threat:

Since the attacker can eavesdrop on the traffic flowing from the MN to the CN, it can easily cause DoS e.g. by sending TCP RSTs.

6.6.1_Effect:

Selective DoS.

6.6.1_Requirement:

This threat is also non Mobile-IPv6 specific and hence no requirement is generated.

6.6.2. Scenario 15

6.6.2_Threat:

Taking advantage of its topological location, the attacker can send BUs to the CN, giving the MN's Home Address. This threat is different from threat 6.6.1.1_Threat in the sense that this attack works even in the presence of fully functioning ingress filtering and even if Alternate CoAs were disallowed.

6.6.2_Effect:

MITM/DoS.

6.6.2_Requirement:

Same as verifying if the sender is authorized to send BUs for the home address contained in the BU.

6.7. Threat model for the case where the MN sends a binding update to the previous router asking it to take on the role of an HA temporarily

Section 10.9 of the Mobile IP specification allows a MN to send a binding update to a router (that can act as a Home Agent) on the previous subnet that the MN was attached to, and request it to forward packets destined to the MNs previous COA to the new COA. The specification also states : "As with any packet containing a Binding Update (see section 5.1), the Binding Update packet to this home agent MUST meet the IPsec requirements for Binding Updates, defined in Section 4.4." However it is not clear how the MN could have

established a security association with that router on the previous subnet.

6.7.1. Scenario 16

6.7.1_Threat:

An attacker who is aware of a MN being currently attached to a subnet could send a binding update to a router on that subnet (which is willing to act as an HA) with the H bit set.

6.7.1_Effect:

This binding update which is spoofed causes the HA router on that subnet to create a binding entry for the legitimate MN to some other COA. It will start intercepting the packets destined to the MN (which is still on the same subnet) and forward(tunnel) it to the COA specified in the binding update. Traffic destined to a MN is now redirected elsewhere causing a DoS attack.

6.7.1_Requirement:

A router on a subnet willing to take on the role of an HA for a MN (even on a temporary basis) MUST establish a security association before the router will accept BUs for a MN with the H bit set.

<Comment 3 in Appendix B>

6.8. Other threats, including those that target the Home Agent

6.8.1. Scenario 17 - Home Agent discovery via the ICMP anycast Home Agent discovery message

> Section 9.2 of the specification [Ref1]: "As described in Section 10.7, a mobile node attempts dynamic home agent address discovery by sending an ICMP Home Agent Address Discovery Request message to the "Mobile IPv6 Home-Agents" anycast address [10] for its home IP subnet prefix, using its care-of address as the Source Address of the packet. A home agent receiving such a Home Agent Address Discovery Request message that is serving this subnet (the home agent is configured with this anycast address on one of its network interfaces) SHOULD return an ICMP Home Agent Address Discovery Reply message to the mobile node (at its care-of address that was used as the Source Address of the Request message), with the Source Address of the Reply packet set to one of the global unicast addresses of the home agent."

The reply message MAY contain a list of all possible home agents on that subnet.

6.8.1_Threat:

An attacker who knows the home address of a MN can possibly send a home-agent discovery message to the MN's home subnet and receive a list of all home agent routers on that subnet.

6.8.1_Effect:

This would expose the structure of the operator's network (to some extent) which is not desirable. It would also allow an atacker to determine the routers acting as home agents and mount DoS attacks or other types of attacks on these routers and thereby cause these routers to be unable to forward packets to MNs that they are intended to serve.

6.8.1_Result:

One of the things that operators might do is to make sure their firewalls do not allow any ICMP home agent discovery messages to be let in. This would defeat the whole purpose of having the ability to do home agent discovery. 2 Use the Home Agent as a packet reflector

6.8.1_Requirement:

An HA which responds to an ICMP home agent discovery message SHOULD only do so after authenticating the MN's identity.

6.8.2. Scenario 18 - HA used as a Packet reflector

6.8.2_Threat:

If an attacker can make a Home Agent to believe that a Mobile Node is at a given CoA, the attacker can then use the Home Agent as a packet reflector when launching a distributed DoS attack against the node at the CoA. That is, by simply sending packets to the Home Address, the Home Agent will tunnel them and send them to the DDoS target. An HA will create a binding entry for an MN if the authentication in the BU is valid. Using the HA as a packet reflector makes it easier for the DDoS attacker to hide itself, making it harder to succesfully shut down the DDoS attack.

6.8.2_Requirement:

The MN and HA MUST have a strong security association and the HA MUST verify the BUs sent by any IPv6 node requesting the HA to intercept packets destined for it and tunnel them to it's COA.

6.8.3. Scenario 19 - CN as a packet reflector

According to the Mobile IPv6 spec: "A node receiving a packet that includes a Home Address option MAY
implement the processing of this option by physically exchanging the
Home Address option field with the source IPv6 address in the IPv6
header."

An attacker can simply spoof the home address option in packets sent to a CN causing the CN to swap the source address with the address contained in the home address option. This causes the CN to become a packet reflector in attacks on nodes whose addresses may be known. Using the CN as a packet reflector may make it easier for the DDoS attacker to hide itself, making it harder to successfully shut down the DDoS attack.

6.8.3_Requirement:

CNs SHOULD NOT/MAY NOT process any packet (BU or not) containing a Home Address option unless they have verified that that the node sending the packets is authorized to use the home address in the destination option.

6.8.4. Threat model specifically in wireless networks

Wireless network technology typically enables security features through its own technology specific techniques. To a greater (GSM) or lesser (802.11) degree these techniques offer some level of security. The network provider must in any case enable these features and it is sometimes the case that this is not done. There are well-known deficiencies in the security schemes of some of the technologies. In general the wireless link may easily become the weakest link in terms of system and network security.

7. Requirements for MIPv6 Security

7.1. General Requirements

A Should be no worse than IPv4 as it is today.

B Should be as secure as if the mobile node was on the home link without using Mobile IP.

C Identity verification MUST not rely on the existence of a gloabl PKI.

D Any solution that is developed for securing the binding updates (MN-HA and MN-CN) should be able to use whatever security associations may already exist to minimize the threats created by on-axis attackers. In particular:

D.1
It is assumed that in all schemes there will be some form of pre-established security association between a mobile node and its home agent. Such a security association should be used to minimize the threats. In this context it makes sense exploring the complexity of handling mobile-to-mobile communication differently than mobile-to-nonmobile communication. As an example, if two MNs are communicating while visiting fairly untrusted visited links, it may make sense to take advantage of the fact that each mobile has a security association with its home agent when exchanging the messages needed to establish the binding. Thus these messages might travel MN1->HA1->HA2->MN2 (and in the reverse direction) so that the risks for a MITM attack are limited to the HA1<->HA2 path.

D.2
In some deployments a PKI may exist (encompassing for e.g some home "domain" which includes a set of MNs, their HAs and some CNs). In that case it should be possible to use the local PKI to prevent MITM attacks when the CN is covered by that PKI. (For instance, if both MN and CN share a trust chain in the PKI sense it should be possible to take advantage of that.)

D.3
If a method to validate public keys (without the existence of CAs and PKI) is created or exists, then it should be possible to take advantage of that mechanism for improved security of the BUs.

7.2. Specific to Mobile IPv6:

0 Security for binding updates is MANDATORY. This is already the case for MIPv6 and as such is not a new requirement. However the mechanism used for securing binding updates MUST be one that is scalable and does not rely on existence of PKIs.

1 It SHOULD be extremely difficult for an attacker "off-axis" i.e. an attacker that cannot snoop packets on either of the three legs of the paths, to divert traffic. This difficulty should be on the order of correctly guessing a very large random number.

2 It SHOULD be possible to leverage the only security association that can be preconfigured (the MN-HA SA) to secure BUs to CNs.

3 It MUST be possible for a mobile node to be anonymous while still taking advantage of route optimization. Thus if a Mobile Node is using RFC 3041 temporary addresses for its home and/or COA it must be able to use a different visible identity when it uses a different temporary address.

4 It SHOULD be possible to negotiate alternative cypher suites/algorithms. It SHOULD be possible to negotiate alternative mechanisms. All implementations MUST implement one designated mechanism and algorithm for interoperability reasons.

5 If IPsec is used as part of the solution it SHOULD not place additional requirements on the set of IPsec SPD selectors beyond what is in common implementations. (Note: This is however debatable. A soon to be published I-D will identify the issues of using IPsec in conjunction with Mobile IPv6.)

6 Router Advertisements sent by the HA to the MN MUST be secured.

7 Scalability of mechanisms using symmetric or asymmetric keys MUST be considered in any solution.

8 SHOULD optimize the number of message exchanges and bytes sent between the participating entities (MN, CN, HA). This is an important consideration for some MNs which may operate over bandwidth constrained wireless links.

9 A CN SHOULD be capable of rejecting BUs sent by a MN. If a CN rejects a BU, the MN SHOULD refrain from sending further BUs to that CN (for a period of time).

10 Any approach MUST consider the scalability issues and computational capabilities of the entities in a mobile environment, especially MNs and CNs. The expense associated with generating keys or public key operations or Diffie Hellman computations SHOULD be accounted for.

7.3. Requirements from Threats

6.1.1.1_Requirement
A correspondent node MUST not update its binding cache on receiving a binding update from any IPv6 node without verifying that the packet was sent by a node authorized to create binding cache entries for the home address carried in the home address option of the BU.

6.1.1.2_Requirement
No Mobile IPv6 specific requirements can be generated from this threat.

6.1.1.4_Requirement
a) An IPv6 node that receives binding updates SHOULD NOT create state
until it has verified the authenticity of the sender.

b) An IPv6 node SHOULD have the capability to reject binding updates.

6.2.3_Requirement
The Mobile Node SHOULD be capable of ascertaining the identity of the access point to which is is attaching and authenticate it.

6.2.4_Requirement
Upon receiving a packet carrying a Binding Acknowledgement, a mobile node SHOULD ensure it trusts the sender of that Binding Acknowledgment.

6.4.2_Requirement
The MN SHOULD be capable of authenticating binding requests. The MN SHOULD/MAY only process binding requests which are originated by nodes that are in the binding update list of the MN.

6.4.3_Requirement
The HA MUST authenticate any binding update received by it before making any changes to the binding cache entries.

6.5.1_Requirement
Any requirements to address this threat is outside the scope of Mobile IPv6 as the threat described above is a generic one. However MIPv6 itself SHOULD not cause further grief in establishing end-to-end security either using IPsec or other mechanisms.

6.7.1_Requirement
A router on a subnet willing to take on the role of an HA for a MN (even on a temporary basis) MUST establish a security association before the router will accept BUs for a MN with the H bit set.

6.8.1_Requirement
An HA which responds to an ICMP home agent discovery message MUST only do so after authenticating the MN's identity.

6.8.2_Requirement
The MN and HA MUST have a strong security association and the HA MUST verify the BUs sent by any IPv6 node requesting the HA to intercept packets destined for it and tunnel them to it's COA.

6.8.3_Requirement
CNs SHOULD NOT/MAY NOT process any packet (BU or not) containing a Home Address option unless they have verified that that the node sending the packets is authorized to use the home address in the destination option.

8. Acknowledgments

We would like to thank feedback from many WG members especially Claude Castellucia, Alexandru Petrescu, Gabriel Montenegro and Francis Dupont for their comments and suggestions to make this document better.

9. References

[Ref1] draft-ietf-mobileip-ipv6-13.txt - Work in progress

[Ref2] draft-nikander-ipng-address-ownership-00.txt - Work in progress

10. Authors's Addresses

Pekka Nikander
Pekka.Nikander@nomadiclab.com

Dan Harkins
dharkins@lounge.org

Basavaraj Patil
Basavaraj.Patil@nokia.com

Phil Roberts
Proberts@megisto.com

Allison Mankin
mankin@isi.edu

Erik Nordmark
Erik.Nordmark@eng.sun.com

Thomas Narten
narten@raleigh.ibm.com

Appendix A. Background

There are two basic ways of securing communications and data. One is to use cryptography. The second one is to protect the communications or data using physical and programmatic means, basically making it infeasible to tamper with the data without the required privileges. In the case of communication, the latter approach means that the actual networking equipment must be physically protected, e.g., through pressurising the cables.

When new functionality is added to a networking architecture, the functionality usually means opening up new possibilities for tampering with some (management) data or communications. That is, some of the physical and/or progammatic means of protection are lowered, thereby creating new security vulnerabilities. In the case of Mobile IPv6, there are two new major issues: the Binding Cache, and node mobility. Basically, in order for Mobile IPv6 to be as secure as the system would be without it, there must be means to protect the Binding Cache against unauthorized

modification, and to provide reasonable protection for the Mobile Nodes against malicious networks and for the networks against malicious Mobile Nodes.

Furthermore, the use of wireless link layers creates new threats. For example, unless care is taken at the link layer, it may be hard for a Mobile Node to make sure that it is actually communicating with the very access router that it thinks it is communicating with. However, these threats are mostly independent of Mobile IPv6, and it is not expected that Mobile IPv6 security would necessarily bring any remedy to them.

When cryptography is used to secure communications, there must be a way of creating a session key. The session key may then be used to protect (some of) the communicated data against eavesdropping and/or unauthorized modification. However, if the communicating parties do not have any direct nor indirect security relationship between them, there are no known methods for creating such session keys in a manner that would be secure against all attackers. (One example of an indirect security relationship is one created with the help of a trusted third party.)

In the case of Mobile IPv6, the main threat we want to protect against is unauthorized creation or alteration of Binding Cache Entries. One way to define who is authorized in this case is to define that whoever "owns" the Home Address is authorized to create Binding Cache Entries for it [Ref2].

Unless the IPv6 addresses are themselves used as some kind of pre-established security relationships, the only other way of providing security relationships between an arbitrary pair of a Mobile Node (MN) and a Corresponding Node (CN) is to create a global trusted third party based security infrastructure. Experience has shown that building such an infrastructure is extremely hard, and not likely to succeed any time in the near term future.

Thus, it seems like it is, in practice, impossible to build a deployable Mobile IPv6 security solution that is secure against all possible classes of attackers. Thus, this document goes into some length and detail in describing threats caused by various classes of attackers, keeping in mind the goal of "no worse than IP v4 with switched Ethernets."

Generic attack descriptions

Here we give a brief overview of the possible attacks.

- In a Masquarade attack a node plays the role of another node towards a third node. That is, if Mallory is able to convince Bob that he is Alice, he is masquarading as Alice. Basically, even in the current IPv4 internet, if Alice is switched off or off-line, it is fairly easy to masquarade as Alice if Mallory are able to eavesdrop or anticipate the traffic flowing back from Bob to Alice.

- In a Man-in-the-Middle (MITM) attack a node plays a double masquarede. That is, Mallory plays Bob to Alice and Alice to Bob. In the current IPv4 internet, if the attacker is on the path between two nodes, or at the same physical link with either of them, there are a number of mechanisms that can be emploeyd to launch MITM attacks. The mechanisms include, for example, tampering with the routing tables and ARP spoofing.

- In a Denial-of-Service (DoS) attack, an attacker prevents a node from communicating with one or more other nodes. For example, Mallory may be able prevent Alice from communicating with Bob, even though they could communicate without the presense and acts of Mallory. A Denial-of-Service attack can either be selective, e.g. disrupting communications between Alice and Bob, generic, e.g. disrupting all communications of Alice, or random, e.g. disrupting some communications of Alice.

In the current IPv4 internet, it is fairly easy to launch a large number of different kinds of Denial-of-Service attacks. Thus, the aim of this draft is to point out some new DoS threats so that they can be potentially addressed.

Appendix B: Question and Discussions

- Comment1:

<Note> If the MN is moving in a rapid manner and changing it's CoA quite frequently as a result, it makes it difficult for the attacker to stay as a MITM. The MN on changing it's CoA will send a new BU to the CN and update the binding cache. Unless the attacker is aware of the MN's movement and changes to CoA, it will be hard to continue to be a MITM (but I guess it depends on what point in the network structure the attacker sits). On the other hand, at least in theory an attacker could just send a continuous stream of Binding Updates, and unless the CN had checks for this

specific condition, most packets would still flow through the attacker. </Note>

- Question1:

Does the fact that a BU can contain alternative CoAs open up further security problems?

</Question> <Comment AUTHOR="Pekka Nikander"> IMHO, no. It is foolish to rely on the source address not being spoofed. Personally, I don't believe that it will be ever possible to mandate ingress PRF filtering everywhere. Thus, from the security point of view, the source address and the Alt CoA should be considered equally trustworthy: both can be spoofed. </Comment> <Comment AUTHOR="BP"> I agree. We should just capture the ability of the MN to send an alternative COA to be used in the creation of the binding entry in the cache of the CN, but note that the same issues that exist for the source address exist for the alternate COA. </Comment>

- Question2:

(Question: What does an IPv6 node do when it has all these entries in its binding cache that have some lifetime associated with them and it is not possible to add further entries in this cache without eliminating some. I guess it would be upto the implementation to figure out ways to delete entries that are not being used or FIFO type of mechanisms).

- Comment 2:

<Comment Author="BP"> An attacker on the same subnet as the HA can do a lot of harm. However it is expected that the home subnet is protected quite effectively and such attacks as described above can only be launched by an insider. </Comment>

<Comment Author="BP"> In the case of wireless (Cellular) networks it is expected that the HA is on a virtual subnet and a mobile node as such is never really on it's home subnet ever. A Mobile node performs deregistration when it is back on it's home subnet, but in a cellular network that home subnet as such does not really exist. A MN may be in it's home administrative domain network but not on it's home subnet. Hence there is always a binding for the MN to some COA. Such HAs will be well protected and an attacker being on the same subnet as the HA would be quite difficult.

</Comment>

- Comment 3:

<Note BP> It is not necessary that the default router that the MN is using be the router that acts as the temporary home agent to forward the packets. The attacker could be on the same subnet as the MN and listen to the router advertisements ad determine the one that has the capability to act as an HA for that subnet. The attack could be launched from the same subnet or from elsewhere. </Note>