Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Mobile IPv6

The purpose of the paper is to familiarize you with the Mobile IPv6 standard, its use, and associated security concerns. The rapid growth in the number of wireless and handheld devices is putting a strain on the current IP protocol, version 4, which is not able to keep pace with the increasing demands brought about by the evolving Internet. This paper first briefly describes the need for a new Internet Protocol and the new version of IP, version 6, and its advantages. Then, mobility within IP networks will be explained...

Copyright SANS Institute
Author Retains Full Rights

AD

Mobile IPv6

Sudha Sudanthi
GSEC Version 1.4b
January 17, 2003

Abstract

The purpose of the paper is to familiarize you with the Mobile IPv6 standard, its use, and associated security concerns.

Introduction

The rapid growth in the number of wireless and handheld devices is putting a strain on the current IP protocol, version 4, which is not able to keep pace with the increasing demands brought about by the evolving Internet. This paper first briefly describes the need for a new Internet Protocol and the new version of IP, version 6, and its advantages. Then, mobility within IP networks will be explained and how the current IPv4 protocol was extended to include mobility, followed by how the new IPv6 protocol integrates mobility and its advantages. The status of IPv6 and Mobile IPv6 will be discussed, followed by a study of a popular new security mechanism for Mobile IPv6.

What is IPv6?

Internet Protocol version 4 has been the dominant Internet Protocol (IP) technology for twenty years, resilient through the exponential growth in the Internet and rapid changes in its related technologies over the decades. But as technology continues to soar in usage across the globe, the limitations of Internet Protocol Version 4 (IPv4) have been causing increasing concern to technology experts around the globe, causing a new version of the Internet Protocol, called IPv6, to be designed.

More addresses

The biggest problem with the Internet Protocol as it exists today is that we are rapidly reaching a point where available network address space is running out. IPv4 allows for about 2^32 or 4,294,967,296 addresses which, mainly due to initial misallocation, has already been completely allocated and therefore, leaves no room for growth. NAT, or Network Address Translation, and CIDR, or Classless Inter-domain Routing, are currently helping to ease the address space problem, but each only provide an intermediate solution to the problem.

NAT allows for the conservation of IP addresses by mapping several local addresses within one network to one global IP address and un-mapping the incoming packets from the global IP address to the appropriate local address, thereby conserving the number of global IP addresses used. CIDR allows for a more flexible way of specifying network addresses that also conserves the number of addresses being used. Original IP addresses were allocated using classes, Class A through Class D, each of which denote different byte portions of the 32-bit IP address to be the network part of the address and the remaining to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

be the host portion. However, having only four classes of addresses is very limiting and very often led to many addresses being wasted since organizations rarely needed the large number of addresses being assigned to them. CIDR was then designed to allow the network and host portions of the IP addresses to be assigned on the bit level, allowing more flexibility and only assigning as many addresses as was needed. However, as mentioned, these solutions only provide a temporarily fix to accommodate the current need for addresses, but do not offer a long-term solution that corrects the problem itself.

The new version of IP, IPv6, offers a more permanent solution, allowing for about 2^128 or 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses. This seemingly limitless number of addresses is exactly what is needed to allow growth for the many new Internet-ready devices that are forecasted to become globally prevalent.

Address Auto-configuration and Host Discovery
IPv6 also allows for *address auto-configuration* and *router discovery*, both of which, as will be discussed later, are important features that allow mobility to be built into the protocol.

Neighbor discovery in IPv6 is how hosts learn of the presence of routers on the network. Rather than wait for routers or neighboring nodes to advertise their presence, as in IPv4, a IPv6 host broadcasts a Router Solicitation message and waits for a response in the form of a router advertisement message.

Auto-configuration allows an IPv6 node to obtain its own IP address by using router solicitations, discussed earlier, to discover the network prefix from the local router and then combining this prefix with its own embedded MAC address to form its own IP address. This feature creates less work for the end user, making renumbering of addresses an easy task and mobility possible.

Optimized Header
The IPv6 header has a new format that is designed to minimize header overhead. This is achieved by moving both nonessential fields and option fields to extension headers that are placed after the IPv6 header. The streamlined IPv6 header provides more efficient processing at intermediate routers.

Built-in QoS
The huge number of routing table entries supported by each router in today's networks is demanding an efficient routing infrastructure to lessen the load. Quality of service in IP is an option that insures that certain important types of traffic get priority handling, a feature that did not exist inherently in IPv4 but added later on in extension to the protocol. IPv6, on the other hands, supports QoS inherently, through the use of a 20-bit field in the IP header called the Flow Label. The flow label allows identification and differentiated treatment of any IP

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

address flow. In addition, in IPv6, there is no fragmentation of packets en route, which is easier to implement and reduces the load on routers.

Protocol Extensibility

The IPv4 options field, used to specify optional Internet-layer information, caused many complications, including an increased IPv4 packet processing time because each router seeing the packet must process all of the options before forwarding the packet on to the next router.

The extension header mechanism in IPv6 was developed to replace the IPv4 options field and provide a more efficient method of specifying options. Unlike IPv4, where the options are part of the IPv4 header, IPv6 extension headers are placed immediately after the IPv6 header. Because they are part of the payload, intermediate routers need not be affected by having to process the extension headers. Also, unlike the IPv4 options that can only support 40 bytes of options, the IPv6 extension headers can be chained together one after another, after the IP header and before the upper layer header, unconstrained by any size other than that of the packet. [6]

Mobility Support

IPv4 was not initially designed with support for mobile users because mobility was not an issue when the Internet began. Mobility was later added as extensions to the IPv4 protocol. However, the IPv6 implementation of mobility was designed into the protocol from the ground up, providing better support and integration with the underlying mechanisms. The advantages of integration of mobility into the base IPv6 protocol will be discussed in detail later.

IP Security: Standardized & Mandated

The lack of real end-to-end security in the IP protocol is becoming a problem today. As with mobility, there are many great extensions to the IPv4 protocol that provide security, such as IPsec and HTTPS, but being that they are not part of IPv4 itself, these extensions are not implemented pervasively. However, IPv6 has security, IPSec in particular, built into the protocol itself. The security mechanisms, to be addressed in detail later, though not perfect, provide better protection against some of the problems that persist in IPv4 today.

What is Mobile IP?

Mobile IP refers to the mobility aspect of IP that allows nodes to move to different networks all over the world while maintaining upper layer connectivity. This is not to be confused with 'portability' that allows nodes to move to different networks all over the world and remain reachable, but upper-layer connections must be disrupted each time the node relocates because it has to obtain and be addressed by a new address at each location.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

What makes mobility difficult?

Mobility is difficult because routing and identification are interrelated in the Internet today. An IP node is identified by its IP address, which consists of a network portion and a host portion. Routing in the Internet today is done using the network prefix of the IP address. If a node moves to another network and maintains the same address, packets will continue to be routed to its old network based on the network portion of the node's IP address and, therefore, will never reach the node at its new location. However, if a node moves to another network and obtains a new address based on the network prefix of the new network, although it will receive all subsequent packets sent to it, it will lose already established sessions with peers from its old network.

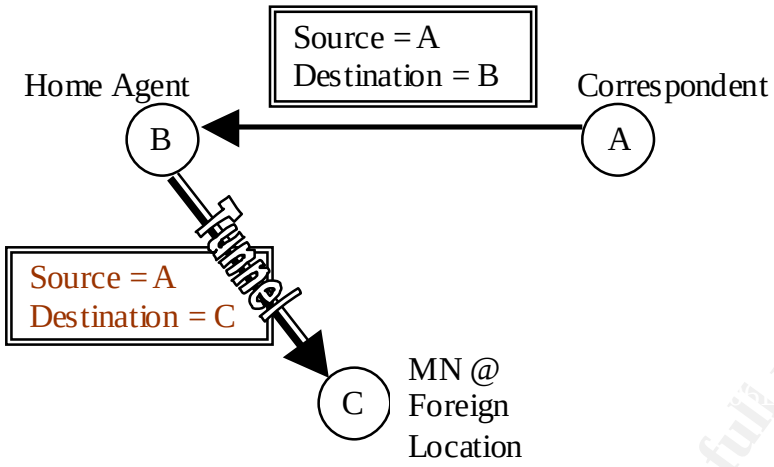
Therefore, the goal of Mobile IP is to allow a mobile node to maintain the same address, regardless of its point of contact to the Internet, in order to maintain existing connections, while remaining reachable at any new location in the Internet.

Mobile IPv4 (MIPv4)

Given that IPv4 was not built with mobility in mind, Mobile IPv4 was designed as an extension to the base IPv4 protocol to support mobility. Mobile IP resolves the issue of mobility by assigning the mobile node a temporary address at each new location, maintaining the MN's original IP address, and, creating and storing a binding between the two addresses with a router in the mobile node's original network.

A *mobile node (MN)* obtains an address in its original location, called *the home address*, and retains this address to maintain end-to-end communication, but also obtains a temporary address, or *care-of-address (CoA)*, from a *foreign agent* (router at a new location) every time it moves to a new network, for routing purposes. The mobile node sends an update, called a Binding Update (BU), containing its new care-of-address to its *home agent* (router in its original network) which allows the home agent to create a binding for the mobile node between its home address and its CoA. Using this binding cache, the home agent intercepts any packets destined to the MN's home address, encapsulates it with its CoA, and tunnels it to the MN at its foreign location.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Thus, via the home agent's binding for the MN, the mobile node is reachable at any location in the Internet using its care-of address and its movement is transparent to the higher layer applications using the home address.

Mobile IPv6 (MIPv6) Advantages

The most significant difference between MIPv4 and MIPv6 is that MIPv6 is integrated into the base IPv6 protocol and not an add-on feature, as is the case with IPv4 and MIPv4. Because most Internet devices will soon be mobile, it is important that all devices are inherently designed to be mobile and IPv6/MIPv6 allows for this. This integrated aspect of IPv6 and MIPv6 also makes MIPv6 more efficient and much easier to implement, the details of which will be discussed.

Movement Detection and CoA Acquisition

Router Discovery and address auto-configuration, discussed earlier as new features in IPv6, makes mobility a much easier task in MIPv6.

When a MN moves to a new network, it can auto-detect its movement based on new Router Advertisements that are being received from a different router or based on the fact that the interval for the expected Router Advertisement from the router with which it was previously communicating was exceeded without another Router Advertisement received. If the latter is the case, the MN can broadcast Router Solicitation messages to invoke a Router Advertisement to be sent immediately from a local router in the new network. Once a new Router Advertisement is received, a mobile node can automatically obtain its new care-of-address (CoA), using auto-configuration based on the prefix advertised in the new Router Advertisement.

Therefore, when a IPv6 mobile node changes location, it automatically detects its movement using Router Discovery and automatically obtains a new CoA using IPv6 Address Auto-configuration. Also, because Router Advertisements may

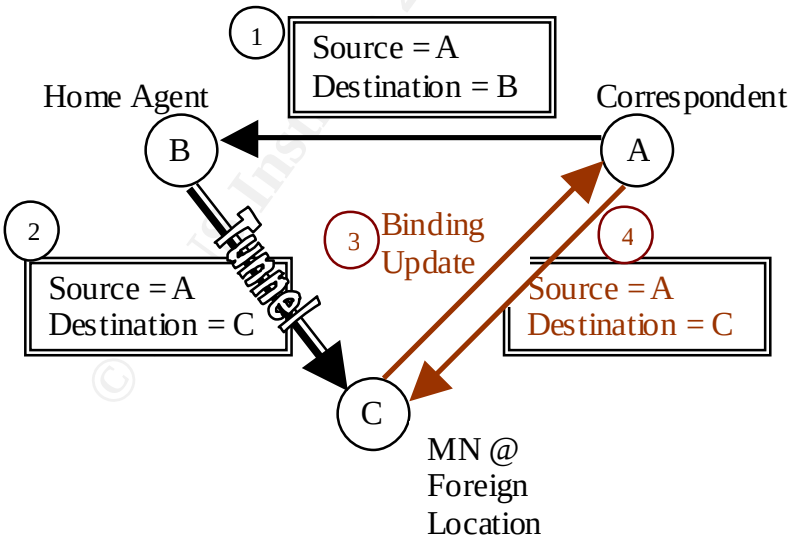
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

come from any router in the network configured to respond to Router Solicitations, and MNs are able to configure themselves based upon these advertisements, MIPv6 eliminates the need for a *foreign agent*, whose function, in MIPv4, was to provide the MN with its CoA and tunnel packets to it received from the home agent.

Route Optimization

As discussed, in the case of Mobile IPv4, when a mobile node changes location, it obtains a CoA and informs its Home Agent of its new CoA and the Home Agent encapsulates and tunnels any packets it receives for the mobile node on its home network to its CoA. Therefore, every time a correspondent node sends a packet to the mobile node, while the mobile node is away from home, packets must first travel to the home network before reaching the mobile node. This inefficient routing is termed triangle routing.

While the Route Optimization capability for all nodes is optional in IPv4, all Mobile IPv6 nodes are designed with this capability. Route Optimization provides the MN the opportunity to eliminate the inefficient triangle routing for any of its correspondent nodes. When the MN receives a tunneled packet from its home agent, it knows that the correspondent node (CN) that sent the original packet is unaware of the MN's current location. Therefore, it may choose to inform the CN of its new CoA using a Binding Update, thereby allowing the corresponding nodes to send packets directly to the MN and avoid triangle routing [14].



Because any IPv6 address can be a mobile node and any IPv6 mobile node may be a correspondent node, every IPv6 node has the capability for Route Optimization. Every IPv6 node supporting Route Optimization dramatically improves network performance when compared to Mobile IPv4 because it

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

reduces the amount of re-routing and tunneling work for the home agent and results in less traffic passing through the home link, reducing bottlenecks at the home link.

IPv6/MIPv6 Status Today

The move towards adoption of IPv6 has been slow in the past, but with the huge success of new, always-on technology and mobile devices, IPv6, with its built-in mobility support, is being widely seen as the necessary next step and steps are currently being taken towards its implementation. The status of IPv6 and MIPv6, including relevant IETF draft and standards, host and router implementations, transitioning method, and the experimental IPv6 network, are discussed here.

IETF Standards

There are a number of IETF standards and drafts that define IPv6 and the MIPv6 aspects of the protocol and attempt to resolve many of their current issues. These documents can be found at the IETF website at www.ietf.org.

IPv6 has been a standard since December 1998 in RFC 2460 and many of aspects of IPv6 are more clearly defined in other proposed standards, a few of these are listed in *Table 1-1*.

Table 1-1: IPv6 IETF RFCs

RFC	*Name*
Internet Protocol Version 6	RFC 2460
Neighbor Discovery for IP Version 6 (IPv6)	RFC 2461
Privacy Extensions for Stateless Address Autoconfiguration in IPv6	RFC 3041
Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	RFC 2463
Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards	RFC 3341

However, because there are many unresolved issues regarding MIPv6, it is still in a draft or proposed standard form. A proposed standard is valid until a certain time, during which time it is reviewed by various universities, organizations, and individuals, then, it is either replaced by a revised proposed standard or deleted. MIPv6, currently on version 19, and its related drafts are all listed in *Table 1-2*. Because most of the MIPv6 proposed drafts listed are expired, they cannot be found at the IETF website, but can be found in various archives in the Internet. They present some of the issues regarding MIPv6 that have been studied and give an indication to the many aspects that are still left unresolved.

Table 1-2: MIPv6 IETF /Drafts

Draft	*Name*	*Expires*
Mobility Support in IPv6	draft-ietf-mobileip-ipv6-19	29 Oct 2002
How to make IPSec more mobile IPv6 friendly	draft-dupont-ipsec-mipv6-01	June 2002
Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents	draft-ietf-mobileip-mipv6-ha-ipsec-01	15 Oct 2002
Fast Handovers for Mobile IPv6	draft-ietf-mobileip-fast-mipv6-05.txt	Sept 2002
Diameter Mobile IPv6 Application	draft-le-aaa-diameter-mobileipv6-02	March 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Mobile IPv6 Authentication, Authorization, and Accounting Requirements	draft-le-aaa-mipv6-requirements-01	May 2002
Localized Key Management for AAA in Mobile IPv6	draft-mun-aaa-localkm-mobileipv6-01	Nov 2002
Hierarchical Mobile IPv6 mobility management (HMIPv6)	draft-ietf-mobileip-hmipv6-07.txt	Oct 2002
Route Optimization in Mobile IP	draft-ietf-mobileip-optim-11.txt	Sept 2001
MIPv6 BU Attacks and Defenses	draft-aura-mipv6-bu-attacks-01	Aug 2002
Securing MIPv6 Binding Updates Using Address Based Keys (ABKs)	draft-okazaki-mobileip-abk-01.txt	Dec 2002
Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6	draft-ietf-mobileip-mipv6-scrty-reqts-03.txt	-
MIPv6 Security: Assessment of Proposals	draft-montenegro-mobileip-mipv6-seceval-01.txt	-
Securing MIPv6 BUs using return routability (BU3WAY)	draft-nordmark-mobileip-bu3way-01.txt	-
Binding Authentication Key Establishment Protocol for Mobile IPv6	draft-perkins-bake-02.txt	-
Security of IPv6 Routing Header and Home Address Options	draft-savola-ipv6-rh-ha-security-03.txt	-
Home Agent Cookies	draft-thomas-mobileip-ha-cookies-01.txt	-

Operating System support

Many vendors currently offer commercial products with IPv6 support for router and end station software. Host MIPv6 implementations include Linux (http://www.cs-ipv6.lancs.ac.uk/MobileIP/) and Microsoft (http://research.microsoft.com/msripv6/). Router IPv6 implementations are several, including Cisco(http://www.cisco.com/warp/public/732/Tech/ipv6/), Hitachi (http://www.hitachi.co.jp/Prod/comp/network/nr60e.htm), and Nortel (http://www.iprg.nokia.com/~hinden/ipv6/). However, because MIPv6 has yet to be standardized, these host implementations vary in the version of MIPv6 draft used in design. For now, these implementations provide a basis for research in helping to study the protocol and its implementations in an effort to build towards better, more complete standards for MIPv6. [7]

IPv6-over-IPv4 tunneling

In addition to MAC addresses being combined with the network prefix to form an IPv6 address, an IPv4 address may be used instead and combined with the network prefix to also form an IPv6 address. On machines that contain both an IPv4 and an IPv6 stack, and this type of IPv6 address, called 6to4 address, connections can be made to other IPv4-only nodes, IPv6-only nodes, or IPv6/IPv6 nodes. This is important because these machines can use IPv6-over-IPv4 tunneling to bridge the gap between existing IPv4 networks and emerging IPv6 networks. Presently, most networks are not native IPv6, but rather, IPv6-over-IPv4, although this is changing constantly and more native-IPv6 networks are being setup.

6Bone

The 6Bone(http://www.6bone.net), or IPv6 backbone, began in 1996 as an experimental, global network made up of several regional 6bones to test the interconnectivity among adopters. The 6bone acts as a testing ground for IPv6 evolution and ultimately assists in helping to migrate towards IPv6. The 6Bone currently consists of various university and corporate research labs who wish to test their IPv6 implementation. Routing in the 6Bone is based on the BGP4

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

protocol and most of the regional 6bones use IPv6-over-IPv4 tunneling, but are evolving towards native IPv6 links.

Mobile IPv6 Security Threats

The security of Mobile IPv6 has been a key issue blocking the standardization of Mobile IPv6. The goal in designing MIPv6 is simply to make IPv6 mobile and at least as secure as MIPv4. However, MIPv6 does introduce several additional security vulnerabilities into IPv6. The biggest vulnerability, and therefore, the one discussed in this paper, is the authorization of Binding Updates (BUs).

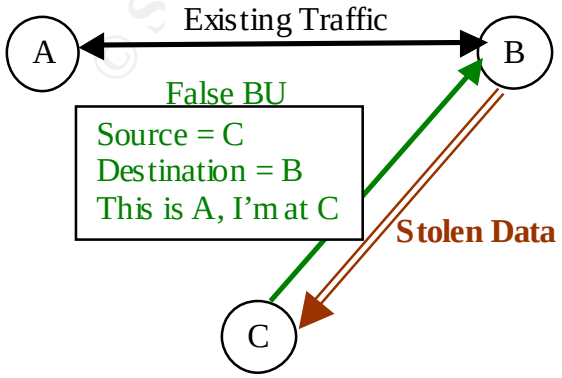
As discussed, MIPv6's Route Optimization is built into the IPv6 protocol rather than added as an extension to the protocol as with Mobile IPv4 and it greatly improves the efficiency of routing by eliminating triangle routing. However, Route Optimization also greatly increases the number of Binding Updates sent by a MN to its CNs, and in doing so, it also greatly increases the security risk of MIPv6.

Unauthenticated or malicious BUs opens the door for many types of attacks, a few of which are discussed here.

False Binding Update attacks

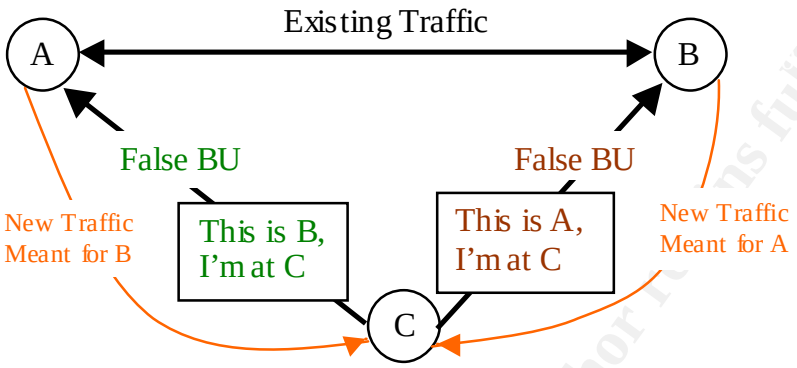
Spoofed Binding Updates may be sent to home agents and correspondent nodes. As every IPv6 node is expected to be deployed as a MIPv6 node as well, and every MIPv6 node is to be a Correspondent Node (CN), BU security threats can been seen as applicable to the whole Internet.

By spoofing Binding Updates, an attacker can redirect traffic to itself or another node and prevent the original node from receiving traffic destined to it. For example, let us say nodes A and B have been communicating with each other, then, an attacker, node C, sends a spoofed Binding Update packet to node B, claiming to be node A with a care-of-address of node C. This would cause node B to create a binding for node A's CoA and subsequent further traffic to node C, believing it to be node A's new care-of-address. Node A would not receive the data it was intended to receive, and, if the data in the packets is not protected cryptographically, node C will be able to see all of node A's sensitive information[3].



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Man-in-the-Middle Attack
An attacker may also spoof BUs to two corresponding nodes in order to set itself as a Man-in-the-Middle between a MN and a CN. For example, if node A and node B are communicating, the attacker could send both nodes a spoofed Binding Update with the care-of-address set to its own address. This would cause both nodes A and B to send all packets to node C rather than to each other.



Without MIPv6's Route Optimization, an attacker would have to be in the path between the nodes in order to capture and read packets.

Denial-of-Service Attack
By sending spoofed BUs, an attacker could also send large amounts of unwanted traffic to overwhelm the resources of a single node or that of a network. The attacker could first find a site with streaming video or another heavy data stream and establish a connection with it. Then it could send a BU to the corresponding node, saying to redirect subsequent data traffic to the attacker's new location, that of an arbitrary node. This arbitrary node would be then bombed with a large amount of unnecessary traffic. Similarly, the attacker could also use spoofed BUs to redirect *several* streams of data to random addresses with the network prefix of a particular target network, thereby congesting an entire network with unwanted data [4].

Mobile IPv6 Security Mechanisms
Mobile IPv6 provides a number of security features that provide protection against many of the threats posed to Mobile IPv6 as a result of its new features. The Mobile IPv6 security features do not attempt to correct security issues that exist regardless of Mobile IPv6. Many drafts exist that address the various security issues within MIPv6, including 'Security of IPv6 Routing Header and Home Address Options' and 'Privacy Extensions for Stateless Address Autoconfiguration in IPv6'.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

However, the biggest security vulnerability of MIPv6, as discussed earlier, is the authentication and authorizing of Binding Updates sent from mobile nodes. There have been many proposals for securing the MIPv6 Binding Updates in the past, including integration of IPSec into MIPv6; however, the key management in IPSec would be too much processing for the IPv6 end devices and, in addition, IPSec depends on PKI which is not widely deployed. Another solution involved using Purpose-Built Keys(PBK) to provide a more lightweight method of authorizing Binding Updates, however, this option does not offer as much security as IPSec. Many other variations of solutions to authorizing binding updates exist and new ones are still being developed, but the dominant solution, designed by the Mobile IP group and documented in the latest IETF Mobile IPv6 security draft, Mobility Support in IPv6, will be discussed here. [10]

The mechanism to ensure security of binding updates between the Home Agent(HA) and Mobile Node(MN) will be briefly discussed, followed by a very detailed discussion of the new method used to ensure the security of binding updates between the Correspondent Node(CN) and the Mobile Node(MN), called the Return Routability Test and Binding Procedure.

It is necessary to first understand a few key terms used in the various security mechanisms. A *node key*, or *Kcn*, is a 20-octet secret, random number held by every correspondent node that helps to identify itself in the keygen tokens that it generates. A *nonce* is a normally 64-bit random number held by each correspondent node and updated at regular intervals. A *nonce index* is associated with each nonce to help the CN identify which nonce, the current one or one of a previous few, was used with a particular message. [11]

Binding Updates between MN and HA

Messages exchanged between the Mobile Node and the Home Agent are protected using IPsec and no new security mechanism exists for this purpose. The use of the mandatory IPSec Authentication Header (AH) and the Encapsulating Security Payload (ESP) and a key management mechanism help to ensure the integrity of the Binding Update messages between the MN and the HA. To prevent the MN from sending a Binding Update for another Mobile Node, the Home Agent must also verify that the Binding Update message contains the correct home address, either as the source of the packet or in an optional field at end of the packet, and the correct security association. [3]

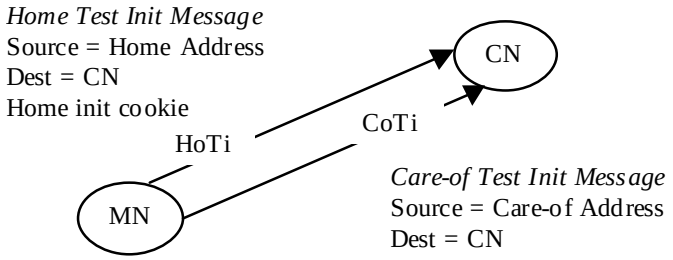
Return Routability Procedure

The Return Routability Procedure provides an infrastructureless method for a CN to verify that the MN is reachable at its home and care-of addresses so that Binding Updates sent from the MN to the CN are secure. The procedure involves two steps where tokens are exchanged between the MN and CN. The MN later uses these tokens to provide verification data in its Binding Update message to the CN. The Return Routability Procedure protects against Denial-of-Service attacks in which an attacker uses the victim's address as its care of

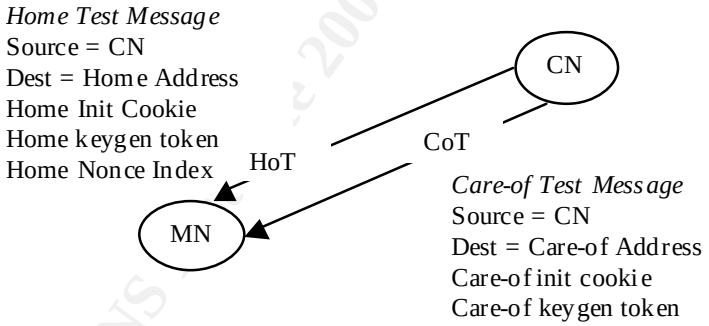
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

address, but it does not defend against attackers that are able to monitor the path between the MN and the CN. [11]

[1] The ***Home and Care-of Test Init* messages**, shown below, are sent at the same time by the mobile node to the correspondent node and they verify that the MN is reachable at its home and care-of addresses and request *keygen tokens* to be sent from the CN. Each message also contains an *init cookie*, a 64-bit random value, which must be returned by the correspondent in the next step to verify the identity of the correspondent node.



[2] Next, the ***Home and Care-of Test Messages*** are sent simultaneously from the CN to the MN, in response to the MN's test init messages, containing keygen tokens.



Included in both messages are the init cookies, which verify that the message is being received by the CN, or at least by a node in the path to the CN.

The CN, upon receiving the Init messages from the MN, generates *home and care-of keygen tokens* from a hash function using the first 64 bits of the MAC, Kcn, home address, and nonce.

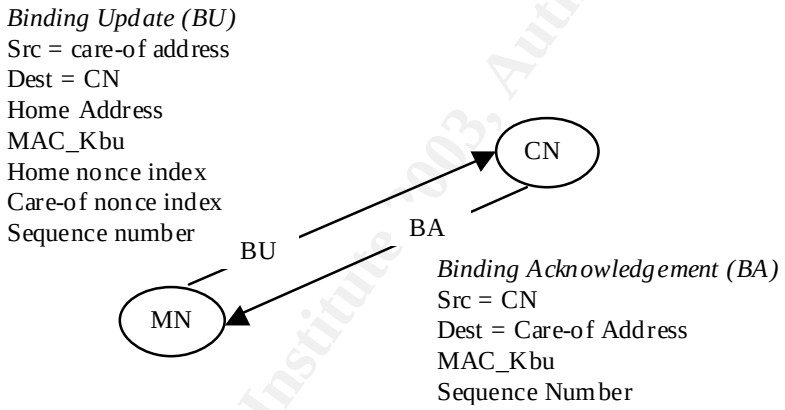
The *home nonce index* is delivered to the mobile node to allow the correspondent node to efficiently find the nonce value that it used in creating the home keygen token.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Binding Procedure
When the MN has received the keygen tokens, the Return Routability Procedure is complete. The MN has the necessary information to send a verifiable Binding Update to the CN. The CN may then reply back with a Binding Acknowledgement if the MN requests it.

Binding Update
When the MN receives the keygen tokens from the CN, it hashes them together to generate the *Binding Management Key* or *kbm*. When sending the Binding Update, it includes its home address, the nonce indexes, sequence number, and the *MAC_kbu*. This new value, the *MAC_kbu,* is calculated by hashing the kbm with a concatenation of the care-of address, CN address, and the entire Binding Update message itself.

Binding Acknowledgement
A Binding Acknowledgement is optionally sent by the CN if the MN requests it. The Binding Acknowledgement contains the same sequence number as in the Binding Update and also contains a MAC_Kbu which is calculated similarly as in the Binding Update, by hashing the kbm with a concatenation of the care-of address, CN address, and the entire Binding Acknowledgement message itself. [11]



Conclusion
The increasing demand for wireless services in recent years is driving the need for a new version of IP that addresses the limitations of the current IP protocol. This new version, called IPv6, with its many advantages, including increased address space, address auto-configuration, and integrated IP mobility, is a promising technology to enable the mobile IP world of tomorrow. The transition to IPv6 is now the obvious solution to a growing problem and this transition process has already begun. And, although Mobile IPv6 has recently been slowed down in standardization due to security issues, these issues will have to continue to get attention, get resolved and integrated into the protocol itself, making every device in tomorrow's Internet, a Mobile IPv6 device, and the Mobile Internet, more efficient, robust, and secure.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Works Cited

[1] Al-Ekram, Raihan. "Mobility Support in IPv6". Waterloo University. 15 Nov 2001. URL:http://www.swen.uwaterloo.ca/~rekram/presentations/mobility_support_in_ipv6.pdf (2 Feb. 2003).

[2] Aura, Thomas. "Designing the Mobile IPv6 Security Protocol". Microsoft Research. 24 Oct 2002. URL:http://research.microsoft.com/users/tuomaura/MobileIPv6/ (2 Feb. 2003).

[3] Aura T., Arrko J. "MIPv6 BU Attacks and Defenses". IETF Draft. Feb 2002. URL:http://www.mit.edu/afs/athena/reference/internet-drafts/draft-aura-mipv6-bu-attacks-00.txt (2 Feb. 2003).

[4] Aura, Thomas. "Mobile IPv6 Security". Microsoft Research. 18 Sept 2002. URL:http://research.microsoft.com/users/tuomaura/MobileIPv6/Mobile-IPv6-Security-18Sep2002.pdf (2 Feb. 2003).

[5] Baptista, Joe. "Overcoming IPv6 Security Threat". CircleID. 12 Sept 2002 URL:http://www.circleid.com/articles/2533.asp (2 Feb. 2003).

[6] Deering, S., Hinden, R. "Internet Protocol Version 6". IETF RFC 2460. Dec. 1998. URL:ftp://ftp.rfc-editor.org/in-notes/rfc2460.txt. (2 Feb. 2003).

[7] "Disruptive Technologies: Technologies that drive IPv6". Ipinfusion. 2002 URL:http://www.ipinfusion.com/pdf/DisruptiveTechnologies.pdf (2 Feb. 2003).

[8] Finney, Joe, McCaffrey. "Mobile IPv6: A Home In Every City?" DMRG, Computer Department, Lancaster University. URL:http://www.newcastle.research.ec.org/cabernet/workshops/radicals/2002/Papers/Finney.pdf (2 Feb. 2003).

[9] "Introducing Mobile IPv6 in 2G and 3G Networks". Nokia White Paper. 2001. URL:http://www.nokia.com/downloads/solutions/operators/intro_to_mipv6.pdf (2 Feb. 2003).

[10] Irava, Venkata S. "Ensuring security of the Binding updates". IETF Draft. URL:http://www.eecs.wsu.edu/~smedidi/Venkata.txt (2 Feb. 2003).

[11] Johnson, David B, Perkins, Charles E., Arkko, Jari. "Mobility Support in IPv6". 29 October 2002. URL:http://ntrg.cs.tcd.ie/htewari/papers/mobicom96.pdf (2 Feb. 2003).

[12] Kato, Tsuguo, Takechi, Ryuichi, Ono, Hideaki. "A Study of Mobile IPv6 Based Mobility Management Architecture". Fujitsu. Sci Tech. J. 37 1 June 2001 URL:http://magazine.fujitsu.com/us/vol37-1/paper09.pdf (2 Feb. 2003).

[13] Lee, Kyeong-Jim Lee. "Mobile IPv6". APAN Penang Meeting. 21 Aug 2001. URL:http://my.apan.net/meeting/downloads/ipv6mipv6-penang-august.PDF (2 Feb. 2003).

[14] Perkins, Charles E., Johnson, David B. "Route Optimization in Mobile IP". 6 Sept 2001 URL:http://www.ietf.org/proceedings/02mar/I-D/draft-ietf-mobileip-optim-11.txt (2 Feb. 2003).

[15] Thompson, Jim. "Mobile Security Flaws Send IPv6 Back to the Drawing Board". ISP-Planet. 09 May 2001. URL:http://www.isp-planet.com/technology/2001/ipv6_now.html (2 Feb. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced