International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Security Overview on Mobile IP Networks

Osama Ali Abdelgadir[1], Amin Babiker A.Nabi[2], Ashraf Gasim Elsid Abdalla[3]

[1]Alneelain University, Department of Electronics & Communication Engineering, Faculty of Engineering
Jamhouria Street, Mugran, Khartoum, Sudan

[2]Alneelain University, Department of Computer Engineering, Faculty of Engineering, Jamhouria Street, Mugran, Khartoum, Sudan

[3]Sudan University of Science and Technology, School of Electronics, College of Engineering
Khartoum, Sudan

Abstract: ***With a rapid growth in wireless technology in recent years, not only have the capacity and performance of wireless communications systems improved exponentially, but also has the range of information and services that can now be accessed using mobile devices. Mobile phones and other handheld devices such as palm pilots, digital cell phones and mobile computing devices allow greatly increasing amounts of information to be retrieved, stored and transmitted in real time. This includes text as well as audio and video data, as illustrated by the ease with which mobile phone users are today able to converse by voice, email or SMS, take and transmit digital photographs, stream audio and/or video files, and upload/download a range of material directly via the internet. Mobile IP has become very important for scientific, humanitarian, military purposes and businesses by providing mobility based on IP addresses using several applications, which keep the communication between devices continue unbroken as the user or node moves from one link to another.***

Keywords: Mobile IP, HMIPv6, FMIPv6, secMIP, DoS

1. Introduction

Since it is connected with each others with critical information and while In mobility, the mobile node changes its location by maintaining the same IP address and keeps connected to the internet, which solves the issue of terminating the communication during handover, so that it has to be secured against many security issues. Since Mobile IP uses open airwaves as a transmission medium, it is faced by many security threats that are extensively in mobile IP networks .Protecting mobile IP from threats and attacks is the most challenging task now a days. This paper Finally describes Mobile IPv6, binding update and associated security concern, basically the common security threats and most effective solutions to protect mobile devices keep connected using mobile in safely. Mobile IP is a protocol developed by IETF, aimed to solve the mobility problem of network node. Mobile IP enables a wireless network node to move freely from one point of connection to the Internet to another, without disrupting the TCP end-to-end connectivity. Mobile IP is built on the IP protocol for internet infrastructure. As Mobile IP is a layer 3 solution for IP mobility, it will suffer from security problems in the same way as IP. As such the issue of securing Mobile IP has become the most significant point with increasing demand on Mobile IP.

2. Mobile IP Functionality

Mobile device first leaves its home network and connects to a foreign network. The agent then sends packets locally to the mobile device visiting that network.

Mobile IP provides transparent Routing of IP datagram over Internet. Each mobile node is identified with its home address regardless of where its current location is. When a node is moved outside its home network as the node associated with a Care-of Address (CoA), which provides information on its current position. Mobile IP specifies how a mobile devices registered with their home agent and how home agent routers connects to the mobile device through a tunnel. Mobile IP provides an efficient and scalable mechanism for roaming over the internet. When using Mobile IP, the devices can change their connection to the internet without changing its IP address. This means that the device can maintain a connection to the transport layer or a higher layer when the device moves and changes its location. A mobile node may have two addresses, a permanent (home) address and a temporary address (care-of address), that changes at each new point of attachment. By using both addresses a mobile computing device can change its location and move to a new network without changing its home IP address and without loosing existing connections. The traffic redirects automatically between the home address and care-of address. There are two versions of mobile IP, Mobile IPv4 and Mobile IPv6. When IP packets are exchanged between a host and mobile device the following steps occurs that are shown in the figure 1:

1) Server x tries to connect to mobile device by sending IP packet with A's home address in the IP header. The IP address is routed to the home network.
2) The home agent intercepts the incoming packet and encapsulates the entire datagram inside a new IP care-of address and transmits the datagram as tunneling to the foreign agent.
3) The outer IP header is removed by the foreign agent and sends the original IP datagram to A through the foreign network.
4) A mobile device receives the message and sends an IP packet to X using X‟s IP address to the foreign agent across the foreign network.
5) The foreign network routes the IP packet to the X server directly across the internet using X‟s IP address.

Figure 1: Mobile IP Operations

3. Mobile IP Security Issues

3.1 A Denial-of-Service Attack

A Denial-of-service attack (DoS) is raised up once the attackers prevent the authorized users from getting their work done. This kind of attack usually takes the following steps:

1) By sending a large number of requests over the internet. These many requests make the target device to run below the optimum speeds till it become unavailable.
2) The other way is to intercept the communication between two devices on the network directly. For example, attacker can use the techniques of redirection to make the data not reach the authorized user.

In the case of Mobile IP, the denial of service attack happens once the attacker starts to manipulate the registration of a care of address for particular mobile device, figure 2 illustrated Denial of Service's manipulated registrations. Such a manipulation of registration leads to two issues:

The Mobile device is no longer connected The attacker gets all the traffic directed to the original mobile device.

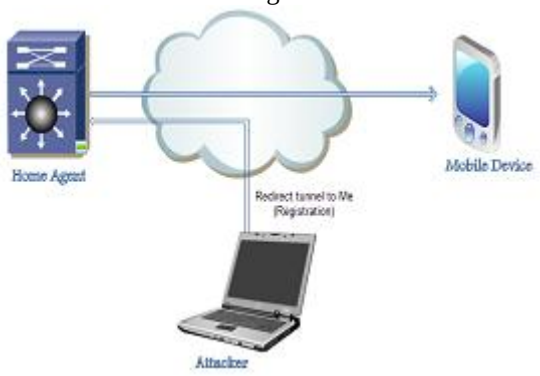

Figure 2: Denial of Service attack to a Mobile IP network

In this kind of attack, the attacker generally needs to be in the middle between the two corresponding hosts in order to cut off their traffic. With a Mobile IP network, the attacker can attack the network from anywhere, if a mobile device is connected on the foreign network, it is mandatory to use the registration method to inform its home agent of its current care-of address to which home agent will intercept and tunnel all the traffic destined to the mobile device's home address. So the attacker can generate a manipulated register request message declaring with its own IP address as the care-of address for a mobile device to the home agent. So all traffic transmitted to the Mobile device goes to the attacker instead. In order to protect the Mobile network from this kind of attacks, strong authentications are required in all registration traffic exchange by a mobile device and its home IP agent.

Authentication mechanism insures that that traffic is going to the mobile device that should receive it, not anybody else. Mobile IP allows a mobile device and home agent to use and agree with any authentication algorithms they agreed. However, all implementation of mobile IP supports the default algorithm MD5 which can provide the strong authentication that is needed.

3.2 Passive Eavesdropping

Passive Eavesdropping is type of a theft of information attack. A passive eavesdropping attack happens when an attacker start to listen to the traffic that is transferred between mobile device and its home agent. The attacker in passive eavesdropping needs to access to the traffic in order this to happen; this can happen in different ways. An attacker can get access to a network and connect a host to the network. In case of a shared Ethernet, all traffic on the same segment may be a victim of eavesdropping. Sometimes a thief is able to receive packets transmitted by radio signals if he is close enough to the wireless network. In order to prevent eavesdropping in mobile IP it is required to use encryption method to encrypt all ongoing traffic information. This can be done in several ways. Traffic should be encrypted on the foreign link, so the attacker can't decode and understand the cipher text and eavesdropping can no longer happen on the foreign link. Although, the traffic still might be a victim of eavesdropping on the rest of end to end connection. The best solution would be to use the end to end encryption method on all traffic, this makes eavesdropping attacks impossible.

3.3 Reply Attack

Using Authentication, a mobile device can prevent the denial of service attack as we mentioned in previous sections. However it cannot protect mobile devices from a reply attack, because the attacker can have a copy of the valid registration request message, buffer it, and then reply it later on by registering a manipulated care-of address for the mobile device.

To prevent this kind of attack, the mobile device has to generate a unique value for identification field of each successful attempt of registration. As such, the stored registration request message by the attacker will be defined as out of date from the respective home agent. Mobile IP defines two ways to set identification field. The first one uses timestamp, where the mobile device uses an estimate date and time of day in the identification field. The second method uses a random number. In this method, the mobile device and home agent declare the value which is entered in the identification field accordingly. A message will be rejected if either device receives a registration message with identification field that not match the expected value and this message will be ignored in the case of the mobile device

3.4 Session Stealing

- Session Stealing is a type of theft of information attacks the same as passive eavesdropping, but in different steps:
- The attacker waits for the mobile device to authenticate and register with its home agent and starts application sessions.
- The attacker eavesdrops on the mobile device to see if any interesting conversation traffic comes through.
- The attacker then floods the mobile device with malicious packets.
- The attacker steals the session by intercepting the packet that is going to the mobile device then the attacker send their own packets that appear to have come from the mobile device.
- The user of the mobile device might not notice that the session has been stolen because there is no sign that something like this has happened. The protection against session stealing is the same as passive eavesdropping by providing end to end encryption with authentication.

3.5 Tunnel Spoofing

The tunnel to the home network or foreign network may be used to hide malicious packets and get them to pass through the firewall. As registration method is a key role of Mobile IP, Mobile IP has some basic security solutions. Mobile IP requires authentication for registration methods between the mobile device and the home agent. Moreover, Mobile IP uses identification fields and timestamp to protect registration from any attacks

4. Security Models

In order to secure the protocol, two approaches can be used:

4.1 Weak Security Approach

Weak levels of security may be used between users in environment such as “campus”, since these services are not high added value or not primarily of commercial nature. A protection against manipulated attempts could be:

- Home Agent assures the care-of address of mobile device is correct, because the allowed care-of address relates to a well known IP address.
- The mobile device in the foreign network has to authenticate bindings.
- When a mobile device attaches to the foreign network, it sends a registration request with password to the home agent.

4.2 Strong Security Approach

The weak security approach that was discussed in the previous section is not suitable any more. Both now have to agree on a stronger level of security policy where mobile IP authenticates any binding message or authenticates information received about a mobile device. Trusted servers and private and public keys are used, but they slow down the operation.

5. Security Improvements of Mobile IP

5.1 Using Tunneling instead of Source Routing

The main purpose of using tunneling techniques instead of source routing is that tunneling relates to fewer security threats. Attacker can use a manipulated care-of address as a destination in a loose source route. This will make the correspondent node reverse the source route and send the message to the manipulated care of address. So the mobile device is disconnected from communicating with his correspondent node. This issue can be solved by proper use of authentication].

5.2 Avoiding Route Optimization

When a mobile device is communicating with a correspondent node from a foreign network, all its packets must be forwarded through its home agent, this is called triangle routing which can results in significant degrading of performance.]Route optimization to mobile IP has been recently proposed, allowing the home agent to inform the correspondent node with the mobile device's care of address, thus correspondent node can communicate directly with mobile device without passing the home agent, which results in less delay and resource consumption. However the main issue with route optimization is security. A network administrator configures a secret key to authenticate between the mobile device and its correspondent node, but with a large numbers of mobile devices, it is not practical to configure keys between a mobile device and every other correspondent node. In the case of triangle routing, it's conceivable to configure a key between mobile device and its home agent.

5.3 Using Firewall

A firewall is used to prevent unwanted access to network services. The firewall monitors the traffic going through the network and decides on the basis of defined rules whether certain packets are allowed through or not. In this way it tries to prevent unauthorized access. Typically, a firewall can not prevent the exploitation of vulnerability in the network service if the communication partner can access it .
There are several kinds of firewall, mainly in the following three categories:

- Packet filtering: It is the oldest network filtering device, introduced on routers. The simple filtering data packet uses the network addresses as basic function of the firewall. It looks at each packet independently and compares it to a list of preconfigured rules. The issue with packet filtering is that it is hard to configure correctly and they cannot keep private IP address invisible to public IP addresses.
- Stateful Inspection: This stateful filtering is an advanced form of packet filtering. It has two main improvements over packet filtering, session table to track all connections and recognition of dynamic application. This make statetful inspection better in protect the internal network from unwanted external access.
- Proxy filter: A proxy firewall is a firewall which is based dedicated proxy and circuit level proxy recourse as filter

modules. These filter modules implement rules by deciding what data is transferred to the actual communication party. In this way it tries to proxy firewall its own network (segment) to protect against unauthorized access, but can also make a conversion of the data cache of certain content, and exercise all other functions that are particular to a proxy.

- In summary, we can say that firewalls provide good security and flexibility for mobile IP by using the firewall categories described above.

6. Threats in IPv6 based mobility services

This section investigates the threats in IPv6 based mobility services. We describe briefly the aim and mechanism of each protocol, then, we identify the main threats originating either from the misuse of the protocol mechanisms or from external mechanisms, out-of the scope of the protocol.

Threats in all IPv6 multihoming solutions

Threats related to all IPv6 Multihoming solutions are discussed in RFC 4218 . This is an informational standard issued by the Network Working Group of IETF in October 2005. We need to consider threats relating to multihoming solutions only if we assume that this is the weakest link in the security of the Internet infrastructure for the multihoming applications. However, it is clear that today, there are other weak links, such as the security of DNS and routing services, and without solving them, the security solutions for multihoming fail. When considering the threats relating multihoming solutions, our assumption is that DNS and routing services function and perform in a by and large trustworthy way.

6.1 Threats for the Traditional Internet Networking

Existing attacks for non-multihoming networks are described in this part. Before them, we highlight the assumptions that are not always explicitly discussed. The assumptions of applications today raise the following problems: Place trust in FQDN reservation to destination IP address (DNS).Place trust in routing (routers, routing protocols), packets are routed to the adversary's IP address. We generally bind cryptographic keying material and SAs to FQDN's or IP addresses, not to the identity of the peers (interruption, perhaps interception, modification, fabrication)

6.2 Threats for non-multihoming networks

6.2.1 Redirection Attack

The redirection of traffic to not the intended address is a threat which can be achieved in Many ways:

Routing: The attacker compromises the routing service by injecting fake long prefix routing information into routing tables, causing non-optimized routing of the traffic on the touched part of the network or leading to routing errors, disruption of traffic.DNS: the adversary modifies DNS forward lookup (IP) (see RFC 3833, Threat analysis of the DNS) leading to fake IP address resolvation, phishing attacks. On-the-path node; an on-the-path attacker can redirect any IP-based traffic, and can intercept, modify and fabricate traffic. To become on-the-path attacker, in case of a public access node, the attacker may inject false Neighbor Discovery or ARP reply messages (ND/ARP spoofing), used to attract all traffic for the legitimate next hop. In this case the attacker was on the same link where the attack happened.

Not-on-the-path node, but between the host and the DNS server: the adversary may modify DNS reply messages to attract traffic. Cause DoS, while not-on-the-path: by false ND or ARP the attacker can cause the honest hosts to believe in a non-existing L2 address. This belief is held for e.g., one minute, until their ARP cache holds the fake L2 address. This can lead to cause a black-hole for the traffic on a link. The internet community is working out state-of-the-art solutions for these problems. These are, e.g., Secure DNS, secure BGP, Secure ND.

6.2.2 Packet injection

Another threat in IP-based networks is the fabrication, i.e., packet injection. The problem is caused by the fact that IP addresses are used as identifier in traditional transport-layer protocols, such as TCP and STCP. If no ingress filtering is applied at the perimeters of the networks, then any source address can be used for the packet, in case of ingress filtering the address space of the subnetwork, where the packet is transmitted from, can be used as source address. Hence, there exists a potential injection of malicious packets for transport-layer or above protocols. The state of-the-art mitigations for the are making difficult to spoof packets by higher layer mechanisms, e.g., in TCP the attacker has to use the correct sequence number and ports. The lifetime of connection, short window size make hard for an off-path attacker to inject acceptable TCP packet. SCTP uses a 32 bit verification tag which has to be known by the attacker to inject a believable packet. IPSec prevents injections by authentication.

6.2.3 Flooding Attacks

Another common threat is the flooding attack, which can also be considered as a redirection attack. Here, the aim of the attacker is to cause DoS, and the attack should not be easily traced back to him. Flooding attacks can be caused in many different ways:

- Reflection without amplification: in this case the attacker induces the resource consumption of other nodes on the network, or the DoS of network services. If the attacker's influence is not amplified by some protocol behaviors, then we speak about a redirection attack without amplification. A TCP Syn attack with spoofed source IP can considered as this type of attack.
- On-the-path attacker: if the attacker is between node A and B, then it can flood A in the following way. Send a TCP Syn to B in the name of A, amplify the requested traffic from B by TCP acknowledgment messages in the name of A, increase the congestion window, and block explicit control messages (Explicit Congestion Notification) from A to B. Any streaming protocol can be used for flooding, if the explicit acknowledgments and feedbacks of the target are forged.

If attacker is not on the path, then the attack can made only in case of lack of ingress filtering at the perimeters of the

network. If there is no ingress filtering, the attacker must be on the path at least at the initialization phase of the flooding attack or the attacker must be able to make a blind setup, i.e., guess all the protecting parameters of the participating parties counter fabrication. For example the attacker needs to guess the initial TCP sequence number of the server.

6.3 Threats for Multihoming Networks

In multihoming network, the attacker has more possibilities to be on-the-path. The time shift between the movement event (real locator change) and the notification of the communicating peers (binding update) open up new potential threat for the communicating parties (mobile node, peer node), in addition, it arises potential DoS threats for all the Internet infrastructure.

6.3.1 Redirection Attack

The attacker can redirect the message flow to:

1) itself: this leads to threats for the confidentiality of the traffic, i.e., interception, or for the integrity of the messages, i.e., modification.
2) to anywhere which is not the destination: these cause threats for the availability, i.e, may cause interruption, DoS for other nodes. Redirection to the attacker is always possible for on-the path attacker. For off-the path attackers this can be executed in the following ways:
   - Once traffic is already flowing: the classic redirection in multihoming can be done. The attacker tries to make a binding update, i.e., make believe for the communicating peer that the location of the attacked node changed. To prevent this attack, the communicating peer should be able to verify, whether the claimed locator really belongs to the claimant.
   - Time-shifting attacks: the attacker is firstly on-the-path, then goes away and launches the attack. For example the attacker can leave in the visited network a bogus ARP entry to cause interruption. The attacker can interrupt ongoing services. After eavesdropping the necessary information, the attacker can move away and launch a DoS attack with spoofed messages. For example, it can send TCP Reset after intercepting the good sequence number, port number, etc.
   - Premeditated redirection: the attacker knows preliminary, that A and B will communicate in the near future. The attacker initiates a connection to B claiming that he is A, at the given location. If the solution to the classic redirection attack is based on "prove you are the same as initially", then A will fail to prove this to B because the attacker initiated the communication. This may cause redirection from A to the attacker, or DoS between A and B. To prevent this attack, the verification of whether a locator belongs to the peer cannot simply be based on the first peer that made contact.
   - Replay: While the multihoming problem doesn't inherently imply any topological movement, it is useful to also consider the impact of site renumbering in combination with multihoming. In that case, the set of locators for a host will change each time its site renumbers, and, at some point in time after a renumbering event, the old locator prefix might be reassigned to some other site. This potentially give an attacker the ability to replay whatever protocol mechanism was used to inform a host of a peer's locators so that the host would incorrectly be led to believe that the old locator (set) should be used even long after a renumbering event. This is similar to the risk of replay of Binding Updates in MIPv6, but the time constant is quite different; Mobile IPv6 might see movements every second while site renumbering, followed by reassignment of the site locator prefix, might be a matter of weeks or months. The solution for these attacks is given by replay protection (fresh nonce), and careful timeout policy for locators.

6.3.2 Redirection to other nodes

Possible attacks to redirect traffic to anywhere on the Internet are as follows:

- Sending packets to a black hole: the attacker can use the classic redirection attack to redirect to a non-existent locator or anywhere on the Internet. The solutions counter redirection to the attacker work also for this case.
- Flooding other nodes by basic third party DoS: in this attack the attacker floods any node on the Internet. The attacker can stay in a slow link anywhere in the Internet. B is on a fast link and A is the victim. The attacker could flood A directly but is limited by its low bandwidth. If the can establish communication with B, ask B to send it a high-speed media stream, then the attacker can presumably fake out the "acknowledgements/feedback" needed for B to blast out packets at full speed. So far, this only hurts the path between the attacker and the Internet. If the attacker could also tell B "I'm at A's locator", then the attacker has effectively used this redirection capability in multihoming to amplify its DoS capability, which would be a source of concern.
- Flooding other nodes by on-path help: in this case, the attacker controls an on-the path node between A and B. The attack is the same as in the previous case, but the on-the-path node injects spoofed acknowledgment messages masquerading as A, and also blocks the trials of A to stop the flooding.
- Privacy related attacks: the use of identifiers make possible defense to some attacks, but also make possible to track the identity. In multihoming solutions, the locators need to be exchanged between the communicating parties. Locators can be wiretapped, eavesdropped, if the multihoming signal control does not provide some privacy protection (e.g., encryption).

7. Identifying Protocols and Mechanisms for Security Threat Analysis

This paper aimed mainly to analyze potential threats in IPv6 based mobility services. This fact leads primarily to the choice of which mobility protocols to be taken into consideration. The analysis focus in the threat-modeling of mobility protocols at the network layer, base don IPv6. The basic protocol in this field is the Mobil IPv6 (MIPv6) protocol that defines a macro-mobility service. All the other mobility protocols in the network layer are the descendants of MIPv6, trying to achieve better variants with less signaling overhead We are interested in the threat-modeling of mobility protocols at the network layer, based on IPv6. The

basic protocol in this field is the Mobile IPv6 (MIPv6) protocol that defines a macro-mobility service. All the other mobility protocols in the network layer are the descendants of MIPv6, trying to achieve better variants with less signaling overhead. The analysis will contain Nemo (Network Mobility) protocol. Moreover, Fast MobileIPv6 (FMIPv6) and Hierarchical Mobile IPv6 (HMIPv6) protocols.

7.1 Network Mobility (Nemo) security threats

Threat of inconsistent routing updates and routing advertisement in the visited network: the MR must not propagate routing advertisements from the home network to the visited network, because it can cause inconsistencies for the routing of the packets in the visited network. Threat of fake Mobile Subnet Prefixes: if an attacker could register inconsistent Mobile Network Prefixes, the HA would advertise and attract traffic destined to these networks, then it would tunnel them to the MR. The MR must check, if the packets arriving on the tunnel interface are destined to one of its Mobile Network Prefixes, as shown figure 3. Otherwise, the Mobile Network would be flooded with false traffic .The disclosure of Mobile Network Prefixes: the attacker could eavesdrop the Mobile Network Prefixes, if they were sent in explicit mode in the Binding Update messages, and there were no confidentiality protection on the bi-directional tunnel. Threat regarding fake Binding Cache Entries: The Binding Update process has to be protected; otherwise an attacker could create false bindings, redirecting the traffic of the CN to itself, or to unsuspicious nodes. The same threats are present than for MIPv6, however, here all the nodes in the mobile network and their CNs are threatened.

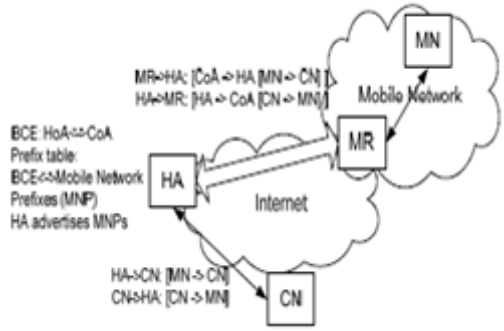

Figure 3: Tunneling in case of NEMO Basic support

7.2 Hierarchical MIPv6 (HMIPv6) security threats

This specification introduces a new concept to Mobile IPv6, namely, a Mobility Anchor Point that acts as a local Home Agent. It is crucial that the security relationship between the mobile node and the MAP is strong; it must involve mutual authentication, integrity protection, and protection against replay attacks. Confidentiality may be needed for payload traffic, but is not required for binding updates to the MAP. The absence of any of these protections may lead to malicious mobile nodes impersonating other legitimate ones or impersonating a MAP. Any of these attacks will undoubtedly cause undesirable impacts to the mobile node's communication with all correspondent nodes having knowledge of the mobile node's RCoA. Malicious Binding Update at the MAP: this threat may lead to the redirection of traffic destined to a given RCoA to a malicious LCoA or to an unsuspected network. The Binding Updates must be protected, only authorized MN should send Binding Updates to MAP. However this limits the scalability, because the MN should have trust relationship or preconfigured security associations with the MAPs. Threats counter the CN: The return routability procedure of MIPv6 can be used also in HMIPv6,as illustrated in figure 4. In HMIPv6 the return routability procedure entrusts the CN that the MN which has a given HoA owns the RCoA at the moment. Without the return routability procedure, the CN would be posed to the same threats as in MIPv6.

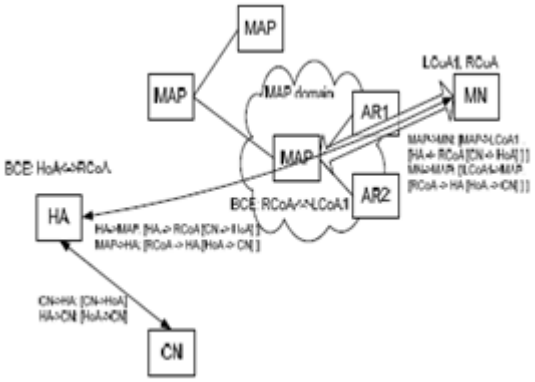

Figure 4: Data transfer in HMIPv6 when it is used together with MIPv6 basic support.

7.3 Fast Handovers for Mobile IPv6 (FMIPv6) Security Threats

Malicious Fast Binding cache entries in PAR: if the FBUs are not protected, the traffic to honest MNs can be redirected to an attacker or to an unsuspecting node or network. All threats which are similar to the MIPv6 Binding update related threats can be imagined, if the FBU is not protected. The standard (RFC 4068) proposes that the origin of the FBUs should be protected by checking at the PAR that the FBU contains a well-formed PCoA. More generally speaking, a mechanism is needed to check that the FBU came from anode that legitimately owns the PCoA. A simple PCoA verification, either it is from the subnet of PAR or not, is not enough for this. The standard also proposes that the FBU may restrict FBUs from L2 addresses, which are in the router's neighbor cache. This would limit the attacker to send FBU messages with spoofed L2 origin addresses. Malicious selection of NCoA: The attacker may send an FBU which binds the subsequent traffic to an NCoA of an unsuspecting node. However, the PAR and NAR are in trust relationship by the assumptions of the protocol, and they can detect duplicate addresses. Threats on the communication between PAR and NAR: The messages between PAR and NAR must be protected because this is the way which assures DAD for NCoAs, and which leads to the creation of binding cache entries in PARs. In case of Reactive Fast Handover, the Fast Binding Update message could be fabricated to make false binding cache entries in PARs, thus redirecting traffic.

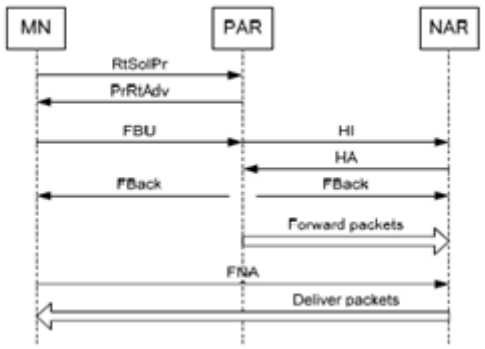

Figure 5: Predictive Handover in FMIPv6.

7.4 Mobile IPv6 Security Threats

Mobile IPv6 has been developed to provide mobility and security for IPv6 with the same features as MIPv4. MIPv6 introduces different security threats as following:

1) Threats against binding updates sent to home agents: an attacker might advise that a certain mobile device is currently at a different location than it really is. Then the home agent accepts the information sent to it as is. The mobile device may not get the message directed to it, and other nodes might get messages they did not want.
2) Threats against route optimization with corresponding nodes.
3) Threat s where MIPv6 correspondent node functionality is used to launch reflection attacks against other parties. The response traffic against a node, whose IP address appears in the option, will be directed using the home address option without giving a possibility for ingress filtering to catch the forged.
4) Threats where the tunnels between the mobile device and the home agent are attacked to make it appear that the mobile node is sending traffic when it is not.
5) Threats where IPv6 Routing Header which is employed in MIPv6 is used to circumvent IP-address based rules in firewalls or to reflect traffic from other nodes. The generality of the Routing Header allows the kind of usage that opens vulnerabilities, even if the usage that MIPv6 needs is safe.
6) The security mechanisms of MIPv6 may also be attacked them, e.g. in order to force the participants to execute expensive cryptographic operations or allocate memory for the purpose of keeping state.

8. Security solutions for IPv6 Based Mobile Networks

8.1 Solutions for all multihoming networks

In general, the aim of securing multihoming solutions is to tie the applied security mechanisms to the identifier of the multihoming node, and not to the locators. The multihoming node should be authenticated based on its identifier. However, this mechanism should not be based on checking previously used locators. Sometimes it is also an aim to check, whether the given identity is really at the claimed location.

8.2 Solutions for MIPv6

The security goal defined at the design of Mobile IPv6 was to provide a solution as secure as the non-mobile IPv4 Internet. Traditional IPv4 gives little protection against on the- path attackers; as a consequence, on-the-path threats, such as disruption, modification, interception remain a residual risk, unless IPSec is used. Still, in case of using IPSec, disruption, denial of service, and redirection of flows are possible.

8 3 Problems with plain IPSec solution

Early in the MIPv6 design process, it was assumed that plain IPSec could be the default way to secure Binding Updates with arbitrary correspondent nodes. However, this turned out to be impossible. Plain IPSec relies on an infrastructure for key management, which to be usable with any arbitrary pair of nodes, would need to be global in scope. Such a global PKI does not exist, nor is it expected to come into existence any time soon. More minor issues that also surfaced at the time were: (1) an insufficient filtering granularity for the state of IPSec at the time, (2) the cost to establish security association in terms of CPU and roundtrip times, and (3) expressing the proper authorization for binding updates. In case of issue (3), it is not enough to authenticate just the identity, but also, to bind the identity to the localization (i.e., current care-of address) in a trusted and verifiable way for the CN. The issues (1) and (3) were addressed between the HA and MN in RFC 3776 . However the lack of global PKI remains unsolved. One way to provide global key infrastructure for mobile IP could be DNSSEC or Secure Neighbor Discovery. These infrastructures are currently worked out. The idea of these architectures is to provide a public certificate for each IP address and sign the binding update by the node having that IP address. However, in order to be secure, each link in such a system must be secure. There must be a chain of keys and signatures all the way down from the root (or at least the common trust anchor of the MN and the CN) to the given IP address. And each signature should explicitly authorize the lower key to manage the corresponding address below. Checking all the signatures on the tree would place a considerable burden on the CN, making route optimization prohibitive, or justifiable only in very particular circumstances. Consequently the obvious question is whether the costs of deploying the global secure DNS infrastructure is worth the additional protection it affords, as compared to simply using return routability for both home address and care-of address verification. The return routability mechanism is the current security solution in Mobile IPv6 route optimization. It was designed to mitigate the threats discussed in the previous section.

The protection level of return routability is close to that of a static IPv4-based Internet. It produces an acceptable cost in terms of packets, delay, and processing. The aim of return routability mechanism is to check, whether the MN is reachable both by home address and care of address. The check yields false positives if the routing infrastructure is compromised or if there is an on-the-path attacker between the CN (verifier) and the address to be verified (CoA). With these exceptions, it is assumed that a successful reply

indicates that there is indeed a node at the given address, and that the node is willing to reply to the probes sent to it. The basic return routability mechanism consists of two checks, a Home Address check and a Care-of address check. These checks are running independently and paralelly. The MN initiates the home address test with a Home Test Init message, and the care-of address test with a Care-of Test Init message. The Home Test Init goes through the HA, the Care-of Test Init goes directly to the CN. Then the CN sends two challenges, as reply for each request, on the same paths where the init messages came. This prevents reflection and amplification attacks. (Note that with fake routing advertisements, IP origin spoofing, these attacks are still possible.) The first challenge is the Home Test, the other challenge is the Care-of Test message.

8.4 Protecting Home Registration

The home registration is the binding update process between the MN and the HA. This is needed for basic mobility support. The standard recommends the usage IPSec extension headers and the Encapsulating Security Protocol (ESP) protocol in transport mode to protect the MIPv6 signaling between the MN and the HA. It must use at least a non-null authentication algorithm which provides data origin authentication, connectionless integrity and optional anti-replay protection. The basic mobility support standard directs the reader to RFC 2406 [58], which describes in details the IPsec ESP protocol. Besides ESP, Authentication Header (AH) protocol could also be used to authenticate the messages between the MN and the HA. This solution is described in RFC 2402 . The MN and HA must establish two Security Associations (SAs), one in each direction. The key management for the SAs can be done in the following ways:

- Static key distribution: keys are distributed off-line, for each MN-HA relation. This must be supported. If Internet Key Exchange protocol version 1 (IKEv1) is used with pre-shared authentication key, then it must be used in aggressive mode.
- Internet Key Exchange (IKE): dynamic key management may also be supported, in a way as described in RFC 2409 [59]. IKE phase 1 credentials must be recognized, (by SPD or MIPv6 processing), to be able to create a new SA in phase 2. If phase 1 identity is FQDN, then secure DNS may be used to trustfully resolve the IP address. MIPv6 is carefully designed to not to send BU before IKE exchange (see 11.3.2 in RFC 3775). The details of protecting signaling between the MN and the HA communication will be described later (based on the standard RFC 3776).

8.5 Protecting Correspondent Registration

MIPv6 supports route optimization (RO) to bypass the HA-MN tunnel and to make a direct communication between the MN and the CN. To achieve this, the CN takes part in mobility management, i.e., it registers routing exceptions for the MN to source route the packets sent originally to the HoA to the CoA. The routing exceptions are stored in the binding cache of the CN for a short life-time. In order to countermeasure the threats regarding and originating from malicious binding updates, the binding update procedure must be protected. In fact, the MN has to provide correct authorization data, which can be obtained via the Return Routability (RR) procedure. The RR is run before sending the BU to the CN. The RR procedure is part of the RO. The RR results in the generation of binding management key (Kbm) at the MN and CN. The key is then used to generate a Hashed Message Authentication Code (HMAC), i.e., HMAC_SHA1, for the authentication and integrity verification of BUs sent by the MN. The HMAC is sent within the BU, and checked by the CN. After successful verification a Binding Acknowledgment (BAck) is sent back to the MN, and the Binding Cache Entry is created in the CN.

8.6 Return Routability procedure

The RR procedure gives assurance to the CN that the right MN is sending a BU. The RR checks that the locator (CoA) where the Binding Update comes from is really possessed by the claiming identity (HoA). RR does not protect against on-the-path attackers. The elements of RR are the following:

- Secret key of the CN (Kcn): it is used internally by the CN to produce nonces for the MN.
- Nonces: fresh nonces are generated in given intervals by the CN. Nonces are stored locally and internally by the CN. The CN also maintains indices for the nonces, and send these indices within the “test” messages. The MN sends back the indexes in the replies. Nonce indices are for indicating cases when the CN refreshes nonce and still gets messages having HMAC signature calculated with previous nonces. Nonces and nonce indices change also when the CN refreshes Kcn.
- Keygen tokens: the CN generate two keygen tokens based on Kcn and the fresh nonce. It uses a HMAC_SHA1 algorithm to compute them. The keygen tokens do not have to be stored locally in the CN, because they can be recalculated when needed. The keygen tokens are sent in two different ways, i.e., directly and indirectly through the HA to the MN. If the MN receives them, it can generate the Binding Management Key (Kbm) used to authenticate the Binding Update.
- Cookies: The home init cookie is sent by the MN to CN in Home Test Init. The care-of init cookie is sent in the Care-of test init message from the MN to the CN. Cookies ensure that parties, who have not seen the requests from the MN, can not spoof replies to the MN. Aim of RR procedure is that the CN obtain some assurance about that the MN is addressable with its CoA and HoA. It accepts BU only at this case. Instructs the CN to direct it traffic from HA to CN directly. The RR tests whether the Home Test and Care-of Test messages, addressed to the CoA and HoA are finally routed to the same MN. MN must give the proof to have received the tokens in the two parallel messages. The MN has to combine the two tokens into one Kbm, and use Kbm to sign the BU.

9. Use of IPSec in Mobile IP

There is more than one proposal and development that investigates the issue of IPsec mobility and security. Zao and Condell proposed a solution to use of IPSec with Mobile IP for connections HA-MN, HA-FA, CN-HA, CN-FA, and MN-CN .IP-IP-tunneling is replaced by IPSec and also some

small adaptations or extensions to the advertisements and registration messages to cope with the IPSec tunnel .

Binkley and Richardson, proposed a way to secure firewall protected area that tolerates Mobile IP or simple mobility systems like DHCP. In this paper they discuss how to use bi-directional.

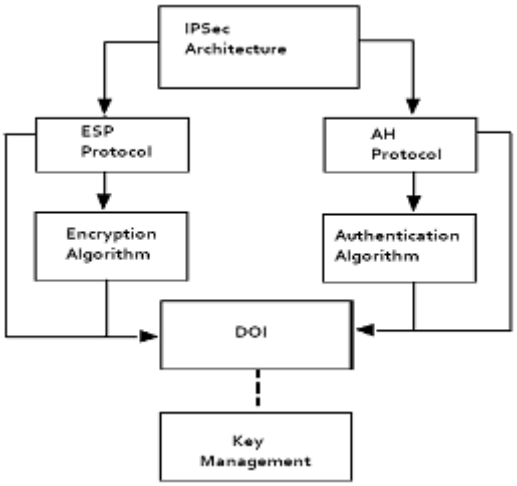

Figure 6: IPSec Architecture

IPSec tunnels between the MN and HA. This scenario is considered as special ad-hoc case where the MN and the HA create a secure ad-hoc network. Another proposal is suggested by V.Gupta and G.Montenegro which considers deployment architecture that describes some enhancements to enable secure Mobile IP operation in the network [29]. These enhancements give the mobile user secure connection in the public network within the firewall-protection. ISAKMP is chosen for key management. Torsten. B and Marc. D proposed a solution called Secure Mobile IP (SecMIP) . They suggest that the interior network is protected by a firewall which acts as the only gate to enter the network. IPSec tunnel will be established between the Mobile IP node and the firewall. The use of SKIP is proposed for key management authentication and encryption . This proposal will be discussed in details later as we consider it as a good solution.

In Mobile IP security, IPSec following features are provided:

- A Tunnel will be created between the two end pairs by using an automatic key and the security association management protocol.
- The use of IPSec ESP protocol in mobile IP by protecting the redirected packets against passive and active attacks.
- IPSec helps the packets to go through firewalls.
- IP-Security and mobility integration.

10. SecMIP (Secured Mobile IP)

Torsten. B and Marc suggest that the idea is to design a new deployment architecture taking the best features of the existing protocols. SecMIP is one of these designs, which stands for Secured Mobile IP. This design is called screened-subnet firewall where the private network is isolated from the outside network (internet) by a demilitarized zone (DMZ), figure 7. The firewall between the DMZ and the private network is the only entry to the private network .

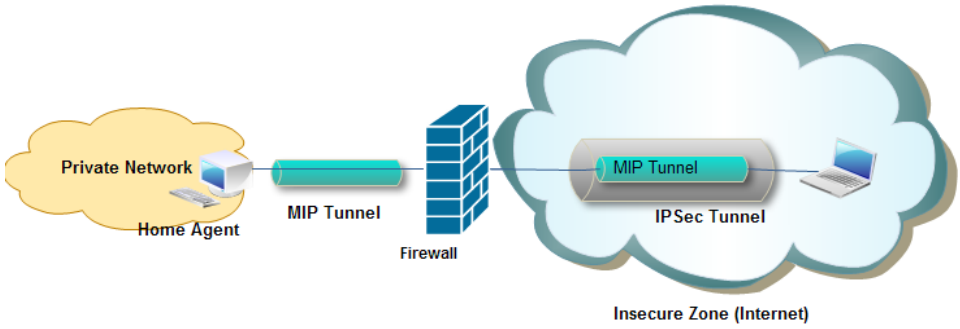

Figure 7: SecMIP tunneling

This architecture simplifies the security management where all the traffic will pass through the firewall, the home agent device is placed inside the private network and all mobile IP nodes must be placed outside (in the DMZ).This provides privacy and protection to the internal network from attacks coming from the internet. The mobile IP node has to authenticate itself to the firewall and this authentication is done by the IPSec protocol. This authentication can be configured with a shared secret or RSA keys. SecMIP uses IPSec tunnel by protecting the mobile IP tunnel where it passes through the insecure outside network (Internet), whereas inside the private network the tunnel is not important. SecMIP uses ISAKMP/Oakley and SKIP, the two are used to provide security for key exchange .ISAKMP is preferred over the SKIP.

11. Summary of threats in MIPv6

In conclusion, there are DoS, MITM, confidentiality and impersonation threats against the parties involved in sending legitimate Binding Updates, and DoS threats against any other party. This is summarized in table 1.

Table 1: Security threats in MIPv6

No	*Attack name*	*Target*	*Security*	*Migrating*
	Basic address stealing	MN's CoA, Any Node's address	High.	RR
,	Future address stealing	MN	Low	RR BCE in lifetime CN
	Attacks against secrecy and integrity	MN	Low	RR, IPsec

	Basic DoS	Any	Med	RR
	Replaying and blocking Binding Updates	MN	Low	BCE lifetime, seq. number MAC
	BCE lifetime, seq. number MAC	Any	High	RR
	Return-to-home flooding	Any	High	RR
	Inducing unnecessary binding updates	MN,CN	Med	Heuristic
	Forcing non-optimized Routing	MN	Low	Heuristic
	Reflection and Amplification	N/A	Med	BU design

12. Conclusion and Future Work

Mobile IP provides network mobility solution over the internet. This paper's study focus on the security aspect in mobile IP and provides a lot of suggestions and methods to improve security in mobile IP. In this report we firstly described wireless network security threats and security technology, we also investigated mobile security threats and different security solutions that can be applied to Mobile IP with emphasis on IPSec to provide the security solution for Mobile IP. Mobility feature and IPSec were not built on IPv4 protocol; they were designed as an extension to IPv4 standard. Mobile IP was an extension of the IPv4 standard under the name "Mobile IPv4" to support mobility. IPSec manages connections and can guarantee both encryption and data integrity through protocols of Authentication Header (AH), Encapsulated Security Payload (ESP) and Internet Key Exchange (IKE). The powerful way to secure mobile IP is by combining it with IPSec protocol; even though there are some limitations such as, IPSec does not stop traffic analysis and it use strong authentication for machines, not users. These limitations can be studied in future work. IPSec is not the only protocol that deal with securing mobile IP, there are several security protocols such as AAA protocol (Authentication, Authorization and Accounting) and Public Key Infrastructure protocol that provide strong management. With a combination of these protocols with IPSec, we get more security and protection for mobile IP. IPv6 was developed because the number of possible address entries in IPv4 is limited. In mobile IPv6, IPSec is a mandatory feature that is required to provide data security and services for communication in IPv6 network. The main difference between Mobile IPv4 and Mobile IPv6 is that Mobile IPv6 is not an add-on feature of IPv6, it is built into the base of IPv6 which makes it more efficient and easier to implement. Mobile IPv6 introduces different security threats that continue to get attention and should be studied in future work.

References

[1] David M. Nicol, "Modeling and Simulation in Security Evaluation," IEEE Security and Privacy, vol. 03, no. 5, pp. 71-74, Sept/Oct, 2005.
[2] John K. Zao, Matt Condell: Use of IPSec in Mobile IP, Internet Draft, November 1997.
[3] V. Gupta, G. Montenegro, Secure and mobile Networking, Mobile Networks and Applications 3 (381-390), Baltzer Science Publisher BV, 1998.
[4] F. Pählke, G.Schäfer, J. Schiller: packet filtering firewall and tunnel configuration to compatible mobility support in IP networks, KiVS 2001, Hamburg, February 2001th
[5] Jim Binkley, John Richardson: Security Considerations for Mobility and Firewalls, Internet Draft, November 1998.
[6] Jian Hui Wang. "Security in Mobile IP" Concordia University, Canada.
[7] Fred Simonds, "Network security: data and voice communications" New York, McGraw-Hill, 1996.
[8] 5 Andrew P. Moore, Robert J. Ellison, Richard C. Linger, "Attack Modeling for Information Security and Survivability", Technical Note, CMU/SEI-2001-TN-001, March,2001.URL:http://www.cert.org/archive/pdf/01tn001.pdf , (checked at 28 September, 2006).
[9] Helayne T. Ray, Raghunath Vemuri, Hariprasad R. Kantubhukta, "Toward an Automated Attack Model for Red Teams," IEEE Security and Privacy, vol. 3, no. 4, pp. 18-25, Jul/Aug, 2005.
[10] ian Hui Wang. "Security in Mobile IP" Concordia University, Canada.