Dr.Chitra Dhawale, Prof.Aumdevi K.Barbudhe, Prof.Vishwajit K.Barbudhe / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 6, November- December 2012, pp.918-921

A Robust Secured Mechanism for Mobile IPv6 Threats

Dr.Chitra Dhawale, Prof.Aumdevi K.Barbudhe, Prof.Vishwajit K.Barbudhe.

Principal, S.P.College P.R.Patil Group of Educational. Institutes, Amravati.
Dr.B.N.C.P.E. Dept.of Computer Science & Technology. Yavatmal.
Agnihotri college of Engineering. Dept. of Electronics &Communication. Wardha

Abstract

Mobile IPv6 has been developed to enable mobility in IP network for mobile terminals. MIPv6 have a lot of feature in comparison to previous Mobile IP protocol . From the data security perspective, the basic objective during the development of Mobile IPv6 has been that it must be at least as secure as previous Mobile IP protocol and it should not introduce any new security threats. But it suffers from various security threats like Eavesdropping, Secure route optimization, connection hijacking and denial of services. and security issues are one of the primary considerations that need to be address. In this paper we proposed a mechanism which includes all security components like Authentication, confidentiality and integrity, secretes key management. It will reduce all security threats and enhance security of Mobile IPv6.

Keywords: Mobile IPv6, Security, Return Routability Protocol, Binding Update, authentication, crypt-ographically generated address.

Introduction

The tremendous advancements in the field of communication and information technology over the last decades have influenced our lives greatly. Mobile IP is a standard protocol established by Internet Engineering Task Force (IETF) and designed to enable mobile users to move from one network to another whilst maintaining their permanent IP address, which gives many advantages to users. The Mobile IP is categorized into IPv4 and IPv6. With the fast growth in the numbers of the mobile and handheld devices that are connected to the internet, the current IPv4 protocol is not able to cover the growth in the number of IP addresses. IPv4 was not built with mobility in mind; Mobile IPv4 was designed as an extension to the base IPv4 protocol to support mobility. 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. Mobile IPv6 is an essential mandatory feature of the IPv6 that has been built to enable mobility for mobile devices in IP networks. Mobile IPv6 specification is still incomplete, so the protocol will most likely have some changes in the future. Security of mobile IPv6 is a essential. Security is one of the most challenging tasks in Mobile IPv6. However, the mobility of communication devices and characteristics of the wireless channel introduce many security issues. And 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. General improvement in MIPv6 may offer enhanced security; however, there are areas still prone to attacks. We proposed a mechanism that integrate all the security enhancing techniques and provide better security to MIPv6.

SEUCRITY ISSUES IN MIPV6

Although MIPv6 is have a lot of features in comparison to MIPv4. But it suffers from various security threats. Some of them are as follows:

A. Secure Route Optimization

To enhance the performance, Route Optimization protocol is used. Route optimization is a technique which enables a mobile node and a correspondent node to communicate directly, bypassing the home agent completely. The concept of route optimization is that, when the mobile node receives the first tunneled message, the mobile node informs correspondent node about its new location, i.e. care-of-address, by sending a binding update message. The correspondent node stores the binding between the home address and care-of address into its Binding Cache. Then after communication directly take place between
MN and CN. The route optimization is not secure because there is no authentication mechanism between MN and CN.

B. Connection hijacking

The connection-hijacking attack is shown in Figure. A, B and C are IPv6 addresses. The Internet nodes A and B are honest and communicating with each other. An attacker at the address C sends a false binding update to B, claiming to be a mobile with the home address A. If

B, acting in the role of a correspondent, believes the binding update and creates a binding, it will redirect to C all packets that are intended for A. Thus, the attacker can intercept packets sent by B to A. The attacker can also spoof data packets from A by inserting a false home-address option into them. This way, it can hijack existing connections between A and B, and open new ones pretending to be A. The attacker can also redirect the packets to a random or non-existent care-of address in order to disrupt the communication between the honest nodes. It has to send a new binding update every few minutes to refresh the binding cache entry at the correspondent.

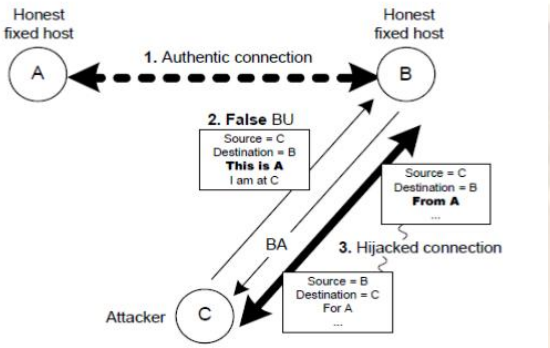

Fig: Connection Hijack Technique

C. Denial of Service

It is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a Denial of Service attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. 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

D. Eavesdropping

Eavesdropping is type of a theft of information attack. It may be passive or active. A passive eavesdropping attack happens when an attacker start to listen to the traffic and get useful information by gathering the session data that is transferred between mobile device and its home agent. In case of wireless network an intruder is able to receive packets transmitted by radio signals. In case of active eavesdropping the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances.

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 solutions exist that address the various security issues within MIPv6. Initially the plan was to use only IPSec Authentication Header (AH) for binding message authentication, without defining and developing any new authentication protocol. This approach encountered many problems and that is why several other methods have also been developed. The current specification defines that IPSec ESP should be used for authentication between MN and HA, and Return Routability (RR) should be used for authentication between MN and CN. The specification makes also possible to use some other, more secure methods than RR for authentication between MN and CN.

1.IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. Messages exchanged between the Mobile Node and the Home Agent is 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 .IPSec can be used to authenticate and encrypt packets at IP level. That is why it was naturally the first proposed method for authentication of the binding messages .The biggest problem with the

IPSec method is the key distribution. Key distribution of the IPSec, which is called Internet Key Exchange (IKE), uses either pre-shared secrets or public keys in the key exchange. After several discussions, IPSec ESP was chosen for binding message authentication between MN and HA instead of IPSec AH.

2.Return Routability Procedure (RRP)

Return Routability (RR) method was developed to provide adequate authentication between a Mobile Node(MN) and a Correspondent Node(CN) .The basic idea in Mobile IP is to allow a home agent(HA) to work as a stationary proxy for a mobile node . Whenever the mobile node is away from its home network, the HA intercepts packets destined to the node and forwards the packets by tunneling them using IPv6 encapsulation to the node's current CoA(Care-of-Address).The Return Routability Procedure provides an infrastructure less 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 it‟s care of address, but it does not defend against attackers that are able to monitor the path between the MN and the CN. First, it ensures that the MN is able to receive messages with its HoA and CoA, after that it protects the binding messages between the MN and the CN. The MN can receive messages with the HoA only if the MN has created a valid binding to the HA in advance.A CN has a private secret key, kcn and a random number, Nj, which it renews atregular intervals. The first and the second message are sent concurrently by the MN to the CN toinitiate the RR method and they contain only the MN‟s HoA and CoA respectively. The first message is sent from the HoA and it is sent via a HA by reverse tunneling the packet first to the HA and then forwarding it to the CN. The second message is sent from the CoA to the CN directly .The third and the fourth messages are sent as responses to the first and the second address respectively. They contain the keys K0 and K1, which are used for authentication of the binding messages, and also the indices of the used random numbers and private keys. The fifth message is the binding update message that is sent by the MN to the CN .It is authenticated by using a secret Kbu, which is calculated with the HMAC SHA1function by using km as a key from the binding message content.The sixth and the seventh messages are optional and they are authenticated basically in the same way as the fifth message .

3.Cry ptographically Generated Addresses

Cryptographically Generated Addresses is an Internet Protocol Version 6 (IPv6) address that has a host identifier computed from a cryptographic one-way hash function. This procedure is a method for binding a public signature key to an IPv6 address in the Secure Neighbor Discovery Protocol .This method is based on the idea that apart of the IPv6 address is derived somehow from the public key of the node. The length of the IPv6 address is 128 bits. It consists of a 64-bit network prefix and a 64-bit interface identifier. The network prefix is used for routing in the network and a specific node in a link is identified with the interface identifier, which must be of course unique in the link. The advantage of this method is that no certificate is needed to convince another node in the network that the address is used by the owner of the public key that is included in the packet .After receiving this message, a CN can now be certain that the message really came from a MN that owns the public key Km by first verifying that the HoA was really derived from Km. The validity of Km can be checked by forming a CGA address from the public key and then comparing the received HoA and the formed address. After that the CN can verify that the MN really sent the message by verifying the signature. The signature can be checked by calculating the hashed value and then comparing it to the one that is recovered from the signature by using the public key Km.

Proposed Security Mechanisms

With the current status of the Mobile IPv6 Security Mechanisms there are still a lot of security flaws to be address. In this paper we proposed a new security mechanism for Mobile IPv6 by integrating the Security algorithm for encryption of message and Secret key which is shared by two communicating parties before and after transmission. Our new proposed technique will be computationally efficient and can also be used to detect, prevent and recover each and every probable threat of Mobile IPv6.It will be able to discriminate unsecured and secured transmission and will provide the total security to Mobile IPv6. It will also provide the technique that will govern the total communication throughout the delivery of data. It can improve the security by providing the extensible supplementary protection in terms of authentication, confidentiality and key exchange.

Conclusion

In this paper, we have discussed Mobile IPv6 and various threats associated with it. These threats prevent secure communication in MIPv6 based nodes. To make the communication secure some methodologies such as IPSec, cryptographically generated addresses etc. are discussed.After studying the current MIPv6 security

mechanism, we proposed the security mechanism that integrate all the security enhancing techniques and provide better security to MIPv6.

References

1. C. Perkins, "Mobile IP: Updated", IEEE Communications Magazine, Volume-40, Number-5
2. C. Perkins, "IP Mobility Support for IPv4: Revised ", Request for Comments – 5944, Internet Engineering Task Force (IETF), November 2010.
3. C. Perkins, Ed., D. Johnson, J. Arkko, "Mobility Support in IPv6" , "A Survey of Mobility Support in the Internet" Request for Comment 6275, Internet Engineering Task Force, July 2011
4. Mobile IPv6 Sudha Sudanthi GSEC Version 1.4b, SANS Institute InfoSec Reading Room
5. R Radhakrishnan, Majid Jamil, Shabana Mehfuz, Moinuddin, "A robust return routability procedure for mobile IPv6", International Journal of Computer Science and Network Security (IJCSNS), volume-8, No-5, May 2008,
6. John K. Zao, Matt Condell "Use of IPSec in Mobile IP", November 1997.
7. Perkins, Charle s E., Johnson, David B. "Route Optimization in Mobile IP". 6 Sept
8. Tuomas Aura, Cryptographically generated addresses (CGA). In Proc. 6th Information Security Conference (ISC'03), volume 2851 of LNCS
9. Qiu Ying; Bao Feng , "Authenticated binding update in Mobile IPv6 networks", IEEE- Conference on Computer Science and Information Technology (ICCSIT), Chengdu, Singapore, July 2010