Journal of Theoretical and Applied Information Technology
15th January 2012. Vol. 35 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NETWORK MOBILITY (NEMO) SECURITY: THREATS AND SOLUTIONS

[1]M. DINAKARAN, [2]Dr. P. BALASUBRAMANIE
[1]Assistant Professor, School of IT & Engg, VIT University, India.
[2]Professor, Department of CSE, Kongu Engineering College, India.
E-Mail: [1]dinakaran_vit@yahoo.com , [2]pbalu_20032001@yahoo.co.in

ABSTRACT

The success of mobile communication, shows that the interest in users to access the Internet or their official networks on the move. This mobility support may be needed for a single user or group of nodes called as movable sub networks. Network Mobility (NEMO) protocol developed by IETF enables the mobile nodes and networks to maintain connectivity to their network or Internet by change their point of attachment to from one access network to another. NEMO is an extension of Mobile IPv6, this works based on tunneling the data from home agent to mobile router. The Quality of Service provided by the NEMO is measured based on the routing mechanism it operates, hand off latency and the way of secured data transfer. Though the tunneling process ensures the security of data, the various nodes involved in NEMO are vulnerable as the network is wireless without a proper infrastructure. This article presents a survey on possible threats and solutions for NEMO protocol and its extensions.

Keywords: *Network Mobility (NEMO), MIPv6, Security.*

1. INTRODUCTION

The demand for Internet access in heterogeneous environments is keeps on increasing, especially in mobile platforms such as trains, buses. The request for connecting with Internet on the move is for entertainment, some times to connect with official network of the mobile users too. In order to support the movable networks, the IETF has been working to develop the basic support protocol called as Network Mobility (NEMO) protocol. NEMO extends the basic end-host mobility support protocol, MIPv6 [1] [2] for providing mobile network support. There are various issues in terminal mobility like routing, hand-off, QoS and security [3] [4] [5]. In NEMO the security mechanisms are needed to ensure secured packet transmission between the Correspondent Node and Mobile Network Node. The Binding Update provides authenticity and integrity to the packets therefore incorrect Binding Update can lead to malicious attacks such as traffic hijacking, denial of service and man in middle attack [6] [7] [8]. The possible attacks in NEMO can be categorized into four types they are [9],

1. Threats related to Mobile prefix and dynamic home agent discovery.
2. Threats related to Binding updates
3. Threats related to the regular packet transfer
4. Threats related to MIPv6 security mechanisms

2. MOBILE PREFIX AND DYNAMIC HOME AGENT DISCOVERY THREATS AND SOLUTIONS

When a mobile node or network joins with a new visited network, the prefix of the mobile node or the visited network may be shared among the router of the visited network and the mobile router. This mobile prefix information may give the important information about the topology of the network and life time of the prefix. This information may be use full to the eavesdrop attackers. In order to be secure on the topology of the network, an authentication mechanism must be introduced before sharing the address prefix for any kind of node. If any visited node requests the address prefix in can be authenticated before sharing the same. This address prefix details can be shared as an encrypted data after authentication.

Dynamic home agent discovery function may be used by the attackers to get the information about the address of the home agents in a particular home network. The home address of the attackers may be use full to the attackers to map the network. An authentication mechanism can be introduced to share

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the home agents address. For additional security DNS Security (DNSSEC) can be used [10].

3. BINDING UPDATES THREATS AND SOLUTIONS

If the mobile node moves out of its home network, it starts searching a new router called access router to provide service from the visited network. With the help of AR the mobile node will maintain connectivity with its home agent. But if the mobile node joins with a new network, topologically it's not possible to maintain the address assigned by the home network. So a new address called Care of Address will be assigned by the AR, then the mobile node has to send an update to its home agent about its new care of address. The process of updating new care of address to the respective home agent or correspondent node is called as Binding Update (BU). This process is implemented once again if the mobile node performs hand off. The mobile nodes duty is to update the new binding always to home agent; it ensures the message integrity between these nodes and assures the home agent about the legitimate mobile node. Binding Acknowledgement (BA) message will be a reply from home agent for the update.

An attacker may claim spoofed information that a particular legitimate mobile node is in different location than where it really is. If home agent believes that information and works based on it, then the respective mobile node may not get the traffic at all. A malicious mobile node may use the home address of a victim legitimate node in forged binding update sent to a correspondent node [11]. These kinds of attacks generate the threats against the confidentiality, integrity and availability of the mobile nodes. An attacker may go through the contents of a packet destined to another node by redirecting the traffic to it. This leads to man in middle attack between mobile node and the correspondent node. An attacker may also send forged binding update with help of current care of address of the legitimate mobile node. The acceptance of such binding update leads to attract the correspondent node's reply and further more the denial of service attack towards the victim node. An attacker may also replay the binding update that the mobile node had sent earlier as an attempt to interrupt its communication. If the replayed old binding update is accepted then the packets towards the mobile node will be sent to its old location, where as mobile node is now in new location. A malicious node related to multiple home agents can create routing loop amount the home agents [12]. This can be attained when a mobile node binds one home address located on a first home agent to another home address on a second home agent. This kind of binding updates will lead the home agents to route the same packets among each as they were not aware of the routing loop.

IPSec ESP provides a secure transfer of BU and BA messages between mobile node and the respective home agent. As IPSec is not assuring about the correct ordering delivery of the message, sequence number can be used to ensure the correct ordering of messages. If at all dynamic keying used for data transfer IPSec can provide anti-replay protection. Replay and reordering attacks are possible if the 16-bit MIPv6 sequence number is cycled or the home agent loses the state related to the sequence number and the same is applicable if the home agent reboots. So, in order to prevent such attacks its better to use dynamic keying, IPSec anti-replay protection and sequence numbers together. A non volatile memory can be used for home agent, so that the state can't be lost.

Generally IPSec associations are bound to the used address. When we use a single pair of manually keyed security, it conflicts with new home address creation for the mobile node or with taking on a new subnet prefix. It's necessary to verify that a mobile node should not send any binding update to another mobile node, though the certificate based automatic keying solves this problem to a certain level. The home addresses in certificate in the subject AltName field in included due to this issue. Still this limits to introduce a new address without automatic or manual procedure to establish a new certificate. Hence, the new home address generation is restricted by this specification to the situations where a security certificate or association for the new address already exists.

When manually keyed IPSec is used, the protection is limited against replay and reordering attacks. If sequence number space is cycled through or home agent reboots or forgets it, then the node is highly vulnerable. The home agent and its mobile node must know the manually configure keys, if this were not in the same domain it's difficult to implement manual keying [13]. The standard block ciphers are used by IPSec in MIPv6 which is not vulnerable to problems associated with manual keying and stream ciphers. The home agent and mobile node must agree on the used keys and rest of the parameters.

The IKEv2 protocol can be used in various scenarios. A mobile node must be restricted to claim

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the home address of another mobile node [14]. Mobile node may negotiate the SA for a particular home address, which can be verified by the home agent that the mobile node is authorized for that home address or not [15]. Policy ingress is expected even with IKEv2 for every home address allocation by the home agent. Including the home address in the Subject AltName field of certificate may avoid this issue; still the implementations may not guarantee to carry the use of a care of address when home address is listed in the certificate. User specific task may be expected in this approach for certificate authority. In IKEv2 the mobile nodes care of address is used to establish SA between mobile and the respective home agent. Hence, new IKEv2 security association is expected if mobile node performs hand off. An optional flag Key Management Mobility Capability (K) is introduced for scenarios that can update the IKEv2 endpoints without reestablishing the security association. The negotiation of cryptographic parameters including Security Parameter Indices (SPI's) and cryptographic algorithms are made automated in IKEv2, thus less configuration information is required. If manual keying is adapted, replay and reordering attacks may affect during the frequent movements in some link layers or deployment scenarios. Numerous or unorganized movement through attached points leads to highly vulnerable, hence IKEv2 can be applied in such cases. In case of high count of mobile node, it's necessary to adopt some automated mechanism to reduce the admin duties to provide security. IPEv2 will be help full in providing better security in such scenarios.

The use of Return Routability procedure provides good support to MIPv6 without any security issues. This procedure verifies the message exchange between the home agent and mobile node's care of address to ensure if both the nodes are reachable [16]. The Binding Update messages are exchanged cryptographically. When symmetric attack is used always the response is sent to the node from where the request has come, which avoids the reflection attack. The correspondent node must wait for authorized binding update form the mobile node. The encapsulation (tunnel) also carried out through encryption between home agent and mobile node with IPSec ESP. Nonse exchange through tunnel avoids the possibility of attackers to verify the nonse message, hence the attack from the visited network can also be prevented.

The return routability mechanism guards the binding update exchanges from all attackers, who are unable to watch the path between the mobile node ant the respective correspondent node [17]. This mechanism doesn't protect against attackers who can monitor the path between HA and CN. DoS attacks can also be protected through return routability procedure.

In regular IPv6 communication the vulnerabilities can be segmented in to three cases,

1. Attackers on the local network of the mobile node and home agent or the correspondent node.
2. Attackers on the path between the home network and correspondent node.
3. Off path attackers from Internet.

Denial of service, masquerading, man in middle, eavesdropping are the general on link attacks in IPv6. These kinds of attacks are possible through spoofing, router discovery, neighbor discovery and some other mechanisms. Cryptographic protection in packets can prevent some of these attacks. With out cryptographic protection the total traffic is highly vulnerable. Off path attackers cannot go though the Internet routing protocols security, hence they will try to deny the service for legitimate users through flooding or reflection attack.

When IPv6 implemented in mobile (MIPv6) with return routability procedure few vulnerabilities are possible [18]. Masquerade and man in the middle attacks are possible in future communications. The life time of binding update may be affected when the BU is sent, if the attacker is on link. Return routability mechanism avoids all off path attackers apart from the regular IPv6, hence vulnerabilities from Internet attackers are prevented. MIPv6 handles vulnerabilities on the home link and correspondent node link in a same way that how IPv6 handles. One merit with IPv6 is that the on path attacker must be on link always, which may not be needed in MIPv6. Some times if the home agent and correspondent node are accessible through wireless LAN, then the links at both the ends are easily vulnerable. Hence layer 2 security mechanism plays a vital role in providing network security in these scenarios.

As sequence number is maintained in binding update the attacker can't replay the same message, hence the participants are prevented from replay attack in return routability procedure. MAC verification will identify the modifications in binding update, so that the modification in BU is also protected. The exhaustion of resources against denial of service attack can be protected by return routability procedure [19]. Keygen tokens from nonce and node keys, which are not specific to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

individual mobile node, are used to send an authentic binding update from the mobile node to the respective correspondent nodes. The correspondent node will reconstruct the keygen tokens based on the care of address or home address through the binding update of the mobile node. Thus memory exhaustion attacks can be prevented at the correspondent node except where on path attackers are concerned. Usage of symmetric cryptography makes the correspondent node to be safe against CPU resource exhaustion attack also.

An attacker may try to fool the mobile node and correspondent nodes to request binding update each other. In some scenarios if correspondent node gets large numbers of binding updates like flooding, this may lead to fail in cryptographic integrity checks. In such scenarios correspondent node can stop processing the binding updates itself. If it finds that its spending more time and resources on processing forged binding updates, it can discard or all binding updates with out even performing the cryptographic operations.

Generally attackers may try to break the return routability procedure in multiple ways. Sufficient 64 bit cookies are used by return routability procedure to protect against spoofed responses. 128 bits of information are used to provide the tokens; this can be an internal input to a hash function. The has function uses HMAC_SHA1 algorithm to produces 160 bit quantity suitable for secured keyed hash of 96 bits length in the binding update. The home keygen token and care of keygen token are the two pieces of 128 bit tokens. It requires very large number of messages, if an attacker tries to guess the correct cookie value. The cookies are valid for short period of time, hence attacker has to maintain high constant message rate which is not possible.

4. PAYLOAD PACKET TRANSFER THREATS AND SOLUTIONS

Payload packets that are exchanged between the mobile node, home agent and the correspondent nodes are has the possibility of threats like in regular IPv6 traffic. But MIPv6 uses the type 2 header, tunneling headers in the payload packets and home address destination option. These mechanisms protect the payload packets against the usual attacks. When the mobile node is not in the coverage, an attacker may forge to tunnel the packets appearing that they are coming from the mobile node to the home agent.

If the mobile node is connected to the correspondent node directly, it will send the payload packets directly. The source address field of the packet's IPv6 header is going to be the current care of address of the mobile node. Hence ingress filter works in usual way even for the mobile nodes as the source address is topologically correct. The mobile nodes home address can be informed to correspondent node through the home address option. The reply is going to be direct to the care of address of the mobile node, if a proper binding update is sent the correspondent node from the mobile node. The attacker may trace the home address option, when the packets are reflected through the correspondent node. Hence it's restricted to use home address option, this prevents reflection attacks which may possible through the home address option. If the IPv6 packet header is managed by IPSec the authentication for home address option is mandatory. Though the authentication is successive, the security of the source address field is not at all compromised.

The Type 2 routing header can be used to avoid viewing the header like in traditional source routing. The source routing header has few security concerns like automatic reversal of unauthenticated source routes and the ability to jump between nodes inside and out side of the network. The security issues are fixed using the type 2 header. The semantics of type 2 header is similar to the special form of IP in IP tunneling where in which the inner and outer addresses are same.

Encrypted tunneling lets the mobile nodes, home agents and the correspondent nodes to protect certain level of traffic analysis. Mobile node and the home agent are expected to have a proper security association that can be used to reliably authenticate the exchanged messages.

5. THREATS AND SOLUTIONS ON MIPV6 SECURITY MECHANISMS

An attacker may attract the legitimate nodes by executing some cryptographic operations or allocating memory in order to keep the state. In this situation the victim node will not have resources left to manage other tasks. Cryptographic protection and verifying the proper usage of source address will protect attacks against tunnel between mobile node and home agent. After a secured binding update the traffic through tunnel is received at the home agent end, it verifies the outer IP address to ensure that it's matching with the current care of address of the mobile node. The outer IP address verification will be useful to prevent the attacker is controlled by ingress filtering and when the attacker doesn't know the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

current care of address of mobile node. If the attacker is not controlled by ingress filtering and the attacker who aware of mobile nodes current care of address can still send traffic to home agent, hence this procedure is weak protection against spoofing of packets that appear to come from the mobile node. If the attacker is on the same link, they can send the spoofing packets with mobile nodes home address as source address with out attacking the tunnel. But this won't affect if the destination of the packet is in the home network. IPSec ESP can be used by the home agents and mobile nodes to protect the payload packets tunneled between themselves. It's always better to use the encrypted tunnels for data transfers.

6. CONCLUSION

In NEMO the security mechanisms are needed to ensure secured packet transmission between the Correspondent Node, Home Agent and Mobile Node. The Binding Update provides authenticity and integrity to the packets therefore incorrect Binding Update can lead to malicious attacks such as traffic hijacking or denial of service. IPsec Transport ESP is used to protect the binding update messages between HA and MN/MR. IPsec provides strong cryptographic components under its architecture. Mobile IP and NEMO are network layer protocols which are built on top of the security strength of IPsec. IPsec is quite secure but it is not properly glued with the rest of the system such that the whole system can be easily attacked by the attackers. IKEv2 protocol also provides better security mechanisms to ensure the confidentiality, integrity and availability of the data.

REFERENCES:

[1] C. Perkins "IP Mobility Support for IPv4", RFC 3344. August 2002.

[2] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[3] J. Mangues, A. Cabellos, R. Serral, J. Domingo, A. Gómez, T. de Miguel, M. Bagnulo. A. García. "IP Mobility: Macromobility, Micromobility, Quality of Service and Security," UPGRADE, Vol. 5 (1), pp. 49-55, February 2004.

[4] P. Thubert, M. Watari, F. Zhao "Network Mobility Route Optimization Problem Statement", RFC 4888, July 2007

[5] P. Calduwel Newton, L. Arockiam, "An Intelligent Technique to Improve Quality of Service (QoS) in Multihomed Mobile Networks", International Journal of Advanced Science and Technology, Vol. 7, pp. 11-19, June 2009.

[6] Timo Koskiahde, "Security in Mobile IPv6"

[7] Khaled Elgoarany, Mohamed Eltoweissy, "Security in Mobile IPv6: A survey", Journal of Information Security Tech Report, Volume 12(1), March 2007

[8] Khaled Elgoarany, Mohamed Eltoweissy, "Security in Mobile IPv6: A survey", Information Security Technical Report, Vol. 12 (1), pp 32-43, 2007.

[9] C. Perkins, D. Johnson, J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[10] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[11] Y. Qiu, F. Zhao, Ed., R. Koodli, "Mobile IPv6 Location Privacy Solutions", RFC 5726, Feb 2010

[12] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[13] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

[14] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol", RFC 4306, 2005.

[15] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, 2005.

[16] Aura, T. and J. Arkko, "MIPv6 BU Attacks and Defenses", IETF Draft, March 2002.

[17] Nordmark, E., "Securing MIPv6 BUs using return routability (BU3WAY)", IETF Draft, November 2001.

[18] Roe, M., "Authentication of Mobile IPv6 Binding Updates and Acknowledgments", IETF Draft, March 2002.

[19] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4225, December 2005.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AUTHOR PROFILES:

M. DINAKARAN has completed his B.Tech (IT) and M.Tech (IT-Networking) in Vellore Institute of Technology, Tamil Nadu and India. He had worked in TATA Consultancy Services as a Assistant System Manager between Sep 2006 to July 2009. He has been awarded as TCS Gems during third quarter of 2008. Currently he is working as Assistant Professor in VIT University, Vellore and he is pursuing Ph. D in Kongu Engineering College, under guidance of Dr. P. Balasubramanie. He has published 10 articles in International Conferences / Journals.

Dr. P. Balasubramanie has been awarded Junior Research Fellowship (JRF) by CSIR in the year 1990. He completed his PhD degree in 1996 at Anna University, Chennai. Currently he is a professor in the Department of Computer Science and Engineering in Kongu Engineering College, Perundurai, and Tamilnadu, India. He has guided 7 PhD scholars and guiding 20 scholars Under Anna University. He has published more than 70 articles in International/ National Journals/Conferences. He has authored 6 books with the reputed publishers.