Mobile IPv6 Security Breaches and Solutions

Ulya Sabeel

Department of Computer Science and Engineering, Amity School of Engineering and Technology
Amity University Haryana
(E-mail: usabeel@ggn.amity.edu)

***Abstract*—**With the fleeting advancement in mobile network communications and modern-day technology, mobile IPv6 has become a very notable research area. It is a standard protocol proposed by Internet Engineering Task Force (IETF) for maintaining a fixed and secure IP address during the communication of mobile device users when they are on-the-go from one network to another. It has been developed to support ubiquitous communication in IP network which consists of many advanced features in comparison to Mobile IPv4.This paper focuses on the security issues in MIPv6 and describes the corresponding preventive measures and technical solutions in providing secure communication without requiring any new security infrastructure.

Keywords*—Binding update, Binding Acknowledgement, Cryptography, Mobile IPv6, Mobile IPv6 Security,*

I. INTRODUCTION

In this paper the Mobile IPv6 protocol that is preceded by older version, Mobile IPv4 has been described. The focus is on describing the security predicaments created by the introduction of mobility and the mechanisms applied for the attack prevention. The security issues can be inimical for the communication of mobile devices and need to be prevented, thus enabling a more robust and secure technology. Mobile IPv6 has resolved the problem of depleting IP addresses and providing advanced features as compared to Mobile IPv4, it would make a dominant network protocol for the next generation mobile networks. Therefore, enhancing the security of such a robust mobility protocol is the need of the hour.

Mobile IPv6 solves the routing problems due to mobility of mobile device users by providing a permanent IP address while the users are in communication. The main purpose of Mobile IPv6 is to cater the host machines effectively and provide the potential path estimates for sending and receiving the packets.

The Mobile IP version 6 consists of the following entities: Mobile Node (MN), Home Agent (HA) and the Correspondent Node (CN) [21], [22], [23]. The MN has a fixed home address (HoA) provided by the Home Network. When the MN moves to a foreign network, it requires one or more new addresses known as Care of Address (CoA). MN registers one of its CoA with the HA such that if a packet is destined for MN's HoA, it can be forwarded to the CoA registered by the MN. The registration process is achieved using Binding Update (BU) message sent to HA [16], [17]. BU contains both HoA and CoA of the MN. The BU message is very crucial for the working of MIPv6 and needs to be secured from attacks [18]-[20]. After HA and CN receive the BU message, HA performs the Binding Acknowledgement (BAck) and sends Binding Requests (BReq) from HA and CN to MN. This binding management process is shown in figure 1**.** The Binding messages are sent to MN's Home Network through the tunnel and finally towards the MN. All data exchange is done through the virtual tunnel between the Home Network and Foreign Network. The packets are encapsulated before sending by the sender i.e. HA with the destination address as CoA of the MN registered. In the Foreign Network, the packets are decapsulated and finally forwarded to the MN.

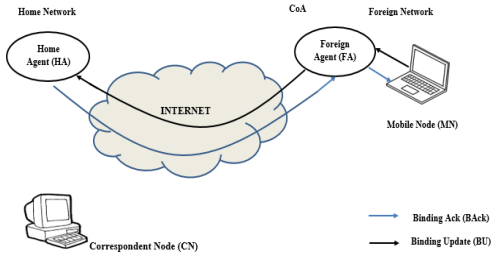

Figure 1: Binding Management Process

This paper is further organized in the following manner. Section II describes the related work. Section III describes the mobile IPv6 security breaches. Section IV describes the solutions to various security breaches in MIPv6. Finally, the study is concluded in section V.

II. RELATED WORK

Mobile IPv6 is a mobility protocol that is defined by IETF in RFC 3775 (obsolete version) [1] and RFC 6275 [2]. It allows the mobile device users to be reachable while they move from one IPv6 network to another [2]. The design for this protocol was based upon the older version, Mobile IPv4 defined in RFC3344[3].

The standardization process for Mobile IPv6 originally started in 1995, but lack of proper security techniques and global authentication infrastructure delayed the standardization process. O'Shea and Roe [7] proposed CAM protocol and Nikander and Perkins [4] proposed the BAKE protocol for enhancing the security in Mobile IPv6 but they proved to be inadequate as proposed by Aura and Arkko in [5]. In [8], the authors proposed some location update protocols based on both CAM and BAKE protocols. But

location update protocols didn't seem that efficient later and some attacks on these protocols were discovered in [6]. In [9] Tuomas Aura, Michael Roe, have explained the threat model and design for MIPv6 security protocol but it is not successful in designing generic strong security solutions. In [10], Timo Koskiahde describes about security in MIPv6 and suggests that as MIPv6 specification is still unfinished, and the security mechanisms proposed might not be enough. In [11], the authors have discussed various MIPv6 security issues and their solutions. These solutions need optimization such that they are more secure and prevent loss of packets. In [12], the authors have discussed the security threats in MIPv6 and their solutions in anycast environment. In [13], the authors have discussed the positive and negative features of MIPv6 security protocols and their underlying design. The authors have proposed their own protocol for BU authentication PKBU. It has low latency requirements resulting in faster handoffs. In [14], Jasmine P. Valera and Sunguk Lee have discussed the security measures for the reduction of security issues in MIPv6. Feng Xiaorong, Lin Jun, Jia Shizhun in [15] have discussed return to routing process, address validation and IPsec mechanism to satisfy mobile IPv6 security requirements.

III. MOBILE IPV6 SECURITY BREACHES

The MIPv6 protocol was designed as a quality extension for the essential IPv6 functionality to be used for communication using mobile devices. Although Mobile IPv6 has a ton of advanced options compared to MIPv4, there are still ambiguities or inadequacies arising particularly in terms of data security. The main objective during the development of MIPv6 is to provide a secure protocol from network or node's standpoint. Some of the security breaches are explained below.

A. Eavesdropping and Man-in-the-Middle attack

Eavesdropping [24] means listening to the conversation between the sender (MN) and receiver (HA) and stealing the sensitive information. This kind of attack can be done actively or passively. During the passive attack, the adversary just listens to the information. During active attack, attacker makes independent connections with the victim and sends fake messages/modified messages to them. The victim is not able to detect that the messages have come from attacker which may create unexpected results [25]. This process is shown in figure 2.

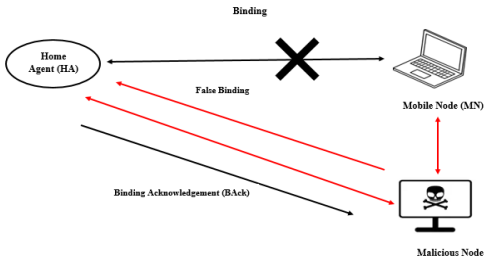

Figure 2: Man-In-The-Middle Attack

B. Stealing Traffic

As the home address of Mobile Node is stored in the DNS, it can be known to anyone. The adversary can steal this information and misuse it for its own benefit. It can also redirect the traffic to itself by sending fake binding update messages to the Correspondent Node as shown in figure 3. The traffic that is meant for MN is stolen by the attacker while it is not even on the path from CN to MN [25].

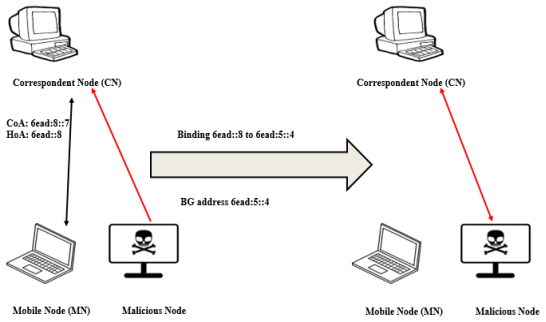

Figure 3: Stealing Traffic

C. Spoofed Binding Update Attack (Impersonation)

In this type of attack, the attackers forge a binding update message and set up a spoofed address as CoA and send the data packets to the fraudulent MN which renders the legitimate MN as non-addressable [26]. The legitimate node not only becomes non- addressable but also loses information. In addition to this, the adversary may also launch DoS attack on the victim by setting the CoA as victim's address and flooding the victim with data from various communication nodes. This may eventually lead to resource exhaustion problem due to overload of data packets at the victim node. This attack is represented in figure 4.

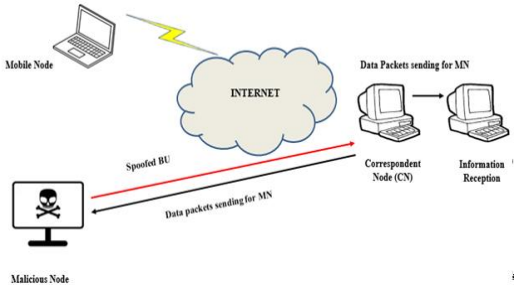

Figure 4: Spoofed BU Attack

D. Connection Hijacking and Traffic Injection

This attack is represented in figure 5. As shown in figure 4, nodes A and B are legitimately communication with each other. The attacker, node C, sends an illegitimate BU message to node B posing as node A. Now node B creates a binding message and redirects all its packets intended for A to C. Now, the attacker can intercept all the packets sent by B to A. The adversary can hijack the existing connection between node A and node B and create new ones posing as node A. The attacker C can also redirect the packets to a random node thus disrupting

communication between the legitimate node and taking over the entire connection set up [9].

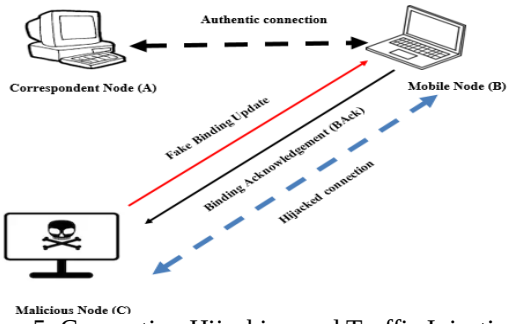

Figure 5: Connection Hijacking and Traffic Injection

E. Denial of Service Attack:

In this type of attack, the attacker sends fake message requests to the server to create unnecessary burden by consuming most of its resources. Because the server is busy, a legitimate node is denied service. In MIPv6, this attack is carried out to deplete CN's memory by sending many fake binding update messages. The CN's memory becomes full and cannot process the messages coming from legitimate clients. Another form of DoS attack in MIPv6 is when the adversary affects or controls the router between the path from MN to CN. This kind of attack is uncommon and very difficult to implement as well as very difficult to prevent [25].

F. Firewall Traversal Issue:

Firewalls that are used quite often in the enterprise networks do not support MIPv6 feature or IPv6 mobility extension headers. If firewalls are used in MIPv6 network, it may lead to discard of BU and BAck messages between the MN and HA because they are secured by Encapsulating Security Payload (ESP), which is not supported by most of the firewalls. During the communication process of MN and CN, if firewall is used, the incoming traffic may not match the existing condition which would lead to packet loss. Firewalls also do not support the MIPv6 feature of bi-directional tunneling. If firewall configuration is modified to support MIPv6 and is not properly configured, it may be susceptible to many attacks like spoofing and DoS [27].

I. Home Address Option Attack:

The MIPv6 protocol supports new headers and options for special data packets. The attackers can make use of this vulnerability and induce hacking hazards into the network. The new address defined by the Home Agent address option is considered to be legitimate. The attackers could use this information for their own benefit and escape the filtering mechanism in MIPv6, thus launching reflection attacks and intercepting data through new Home Address options [28].

J. MIPv6 Routing Header Attack:

In MIPv6, the Routing Header type 0 defines the destination node for the packet arrival. The next address mentioned in the routing header is the address of the next destination node during the data packet transmission. In this way the transmission path is specified between the source to destination. The Routing Header 2 carries the MN's home address information. The adversaries use this information illegitimately and hide the actual destination node address by implementing address redirection and information interception to reflect traffic from other nodes.

K. Dynamic Mobile Prefix Discovery Mechanism attack:

In Mobile prefix discovery mechanism, MN when in the foreign network could get dynamic updates about the configuration and topology changes in its home network [29]. The adversaries in the communication path of MN and HA can listen to this information through eavesdropping or man-in-the-middle attack. They can even change the contents of the prefix data message thus resulting in MN losing its addressing feature.

IV. SOLUTIONS TO VARIOUS SECURITY BREACHES IN MOBILE IPV6

Several security measures and solutions have been proposed to overcome the existing problems in MIPv6. Although these solutions provide secure communication, yet all of them do not guarantee optimized communication. Some of them have been mentioned below:

I. IPSec (IP Security Protocol)

IPSec is a security protocol used during data transmission and protect data integrity to ensure reliable communication. As the authentication and encryption of packets is done at IP level, therefore, it can be used for authentication and encryption of binding messages. IPSec uses the key distribution technique known as IKE (Internet Key Exchange) which uses secret or public key exchange algorithms. The Authentication Header (AH) protocol can be used for message validation to verify that the Binding Update message has come from a legitimate source. Encryption of data is carried out by Encapsulating Security Payload (ESP) that ensures the confidentiality of the messages between MN and HA and prevents the attackers from stealing the information. IPSec guarantees secure communication and helps to prevent the attacks such as Eavesdropping, Man-in-the-middle, Session Hijacking, Spoofed binding update, Traffic Injection and Denial-of-Service.

II. Return to routing (RR) process for Secure Route Optimization

This method provides adequate authentication between CN and MN [30], [31]. The main aim is to protect the binding messages

between MN and CN. CN needs to verify the MN's Home Address (HoA) and Care-of-Address (CoA) before initiating communication with the MN and sharing the Binding Update message (BU). In this method, Home Test Initiation (HoTI) message and Care-of-Test Initiation (CoTI) message are both sent simultaneously by the MN to CN through HA. When CN receives these messages, it creates two cookies combined with its own secret key and nonce value. This information is inserted back in HoTI and CoTI acknowledgement messages and sent back to MN. When the MN receives this information, it creates a fingerprint value to form a session key that is later used to authenticate the Binding Update message sent to CN. When CN receives this message with the session key, it verifies the information using its cookies and creates a binding cache entry for MN. A Binding Acknowledgement (BAck) message may later be sent by the CN to MN to acknowledge the receipt of information. The flow diagram for return to routing process in given in figure 6.

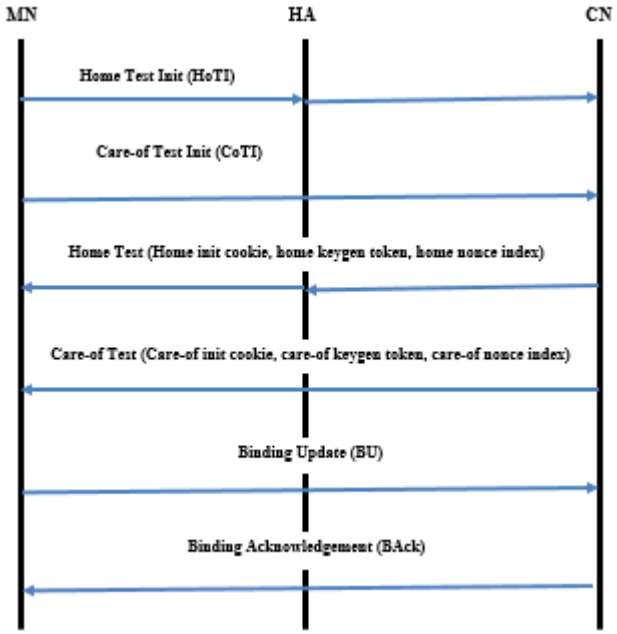

Figure 6: Flow diagram for return to routing process

III. Home Address option and Routing header verification process

To prevent the illegal use of HoA option, stringent verification techniques need to be employed. When the BU message is sent from MN to CN, the address is compared with the source address in binding cache. If it matches, the BU message has come from a legitimate source else the message is discarded.
Router Header Verification process is initiated by RHT2 to ensure that the packets reach an authentic destination. To mitigate the routing header attack, MN's strict verification method must be used. When the MN needs to send data to CN, it, first must check the authenticity of the address. The address is compared to the corresponding address in the binding cache. It the address matches, the routing header address is used in place of destination address in the fundamental headers.

IV. Cryptographically Generated Addresses (CGAs)

This technique is used for the authentication of MIPv6 addresses [32] and provides medium level of security. A 64-bit one-way fingerprint (hash value) of the sender node's public signature key is calculated. The sender node then signs its location information with the corresponding private key and sends public key along with the signed data. The receiver node generates the fingerprint for the public key and compares its value to the address before signature verification on the location data. This averts anyone except the node itself from sending location updates for its address. This technique is based upon the public key authentication without the need for any infrastructure and trusted third parties. The MN signs the BU message and attaches its public key with the message before sending. Once received, the CN can verify that the message has been sent by the legitimate sender.

V. CONCLUSION

The advanced characteristics in MIPv6 have probable security risks. The routing options, the packet header, the binding update messages are vulnerable to different kinds of security attacks. This paper focuses on various security breaches associated with MIPv6 and their possible solutions. To protect data integrity in MIPv6 communication, the security solutions like IPSec have been introduced. The security for the registration of nodes is handled by return to routing process. The validation of home address option and routing header needs to be maintained to ensure the legitimate source address. To authenticate the sender and receiver address, CGAs technique has been discussed. These methods ensure the secure communication in MIPv6. In future, these methods can be optimized to reduce the number of packets lost and decrease the complexity.

REFERENCES

[1] https://tools.ietf.org/html/rfc3775

[2] https://tools.ietf.org/html/rfc6275

[3] https://tools.ietf.org/html/rfc3344

[4] Pekka Nikander and Charles Perkins, Binding authentication key establishment protocol for Mobile IPv6. Internet Draft draft-perkins-bake-01, IETF Mobile IP Working Group, July 2001. Archived at http://www.watersprings.org/pub/id/draft-perkins-bake-01.txt

[5] Tuomas Aura and Jari Arkko, MIPv6 BU attacks and defenses. Internet Draft draft-aura-mipv6-bu-attacks-01, IETF Mobile IP Working Group, February 2002. Archived at

http://www.watersprings.org/pub/id/draft-aura-mipv6-buattacks-01.txt

[6] Tuomas Aura, Pekka Nikander and Gonzalo Camarillo. Effects of mobility and multihoming on transport-protocol security. In Proc. 2004 IEEE Symposium on Security and Privacy (SSP'04), Berkeley, CA USA, May 2004. IEEE Computer Society.

[7] Greg O'Shea and Michael Roe, Child-proof authentication for MIPv6 (CAM). ACM Computer Communications Review, 31(2), April 2001.

[8] Michael Roe, Tuomas Aura, Greg O'Shea and Jari Arkko, Authentication of Mobile IPv6 binding updates and acknowledgments. Internet Draft draft-roemobileip-updateauth-01, November 2001.

Archived at http://www.watersprings.org/pub/id/draft-roe-mobileip-updateauth-01.txt

[9] Tuomas Aura, Michael Roe, Designing the Mobile IPv6 Security Protocol, Microsoft Research, Technical report, April 2006.

Archived at https://www.microsoft.com/en-us/research/publication/designing-the-mobile-ipv6-security-protocol/

[10] Timo Koskiahde, Security in Mobile IPv6, Tampere University of Technology, April 2002, Archived at http://www.cu.ipv6tf.org/pdf/mipv6_security.pdf

[11] Arun Kumar Tripathi, Anchal Srivastava,Harish Pal, Somendra Tiwari, Sukrati Pandey Security Issues in Mobile IPv6, Proceedings published in International Journal of Computer Applications® (IJCA), National Conference on Development of Reliable Information Systems, Techniques and Related Issues (DRISTI) 2012

[12] Amrit Ghosh, Prasun Chakrabarti, Pierluigi Siano, Approach towards realizing the Security Threats for Mobile IPv6 and Solution Thereof, International Journal of Computer Applications (0975 – 8887) Volume 90 – No 10, March 2014

[13] Hero Modares, Amirhossein Moravejosharieh, Rosli Bin Salleh, and Jaime Lloret, Enhancing Security in Mobile IPv6, ETRI Journal, Volume 36, Number 1, February 2014

[14] Jasmine P. Valera, Sunguk Lee, Security Measures in Overcoming Mobile IPv6 Security Issues, International Journal of Database Theory and Application Vol.9, No.7 (2016), pp.297-304 http://dx.doi.org/10.14257/ijdta.2016.9.7.26

[15] Feng Xiaorong, Lin Jun, Jia Shizhun, The Research on Mobile IPv6 Security Features, 2013 IEEE Symposium on Wireless Technology and Applications(ISWTA), September 22-25, 2013, Kuching, Malaysia

[16] D. Johnson, C. Perkins, and J. Arkko, "IP Mobility Support," Internet Engineering Task Force, RFC 2002, Oct. 1996.

[17] S. Robert, "Introduction to Mobile IP," Institute for Information and Communication Technologies, Mar. 2003. http://www. stephan-robert.ch/attachments/File/Networking/MIP_sr_3_03- v2.pdf.

[18] J. Arkko et al., "Secure Neighbor Discovery (SEND)," Internet Engineering Task Force, RFC 3971, Mar. 2005.

[19] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," Internet Engineering Task Force, RFC 3776, June 2004.

[20] K. Sahadevaiah and R.P.V.G.D. Prasad, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks," *Netw. Protocols Algorithms*, vol. 3, no. 4, 2011, pp. 122-140.

[21] J. Arkko, C. Perkins, and D. Johnson, "Mobility Support in IPv6," Internet Engineering Task Force, RFC 6275, July 2011.

[22] K. Ren et al., "Routing Optimization Security in Mobile IPv6," *Comput. Netw.*, vol. 50, no. 13, Sept. 15, 2006, pp. 2401-2419.

[23] A.S. Sadiq, K.A. Bakar, and K.Z. Ghafoor, "A Fuzzy Logic Approach for Reducing Handover Latency in Wireless Networks," *Netw. Protocols Algorithms*, vol. 2, no. 4, 2010, pp. 61-87.

[24] Qiu Ying; Bao Feng,"Authenticated binding update in Mobile IPv6 networks", IEEE- Conference on Computer Science and Information Technology (ICCSIT), Chengdu, Singapore, ISBN: 978-1-4244-5537-9, July 2010, Pages: 307 – 311.

[25] H. Soliman, *Securing Mobile IPv6 Signaling*, Boston, MA, USA: Addison-Wesley, 2004.

[26] Fuliang Li, Changqing An, Jiahai Yang etc, "Investigating the Efficiency of Fine Granularity Source Address Validation in IPv6 Networks", the 13th Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1-8, 2011.

[27] https://tools.ietf.org/html/rfc4487

[28] Baig Z.A., Adeniye, S.C., "A Trust-based Mechanism for Protecting IPv6 Networks against Stateless Address Auto-configuration Attacks", the 17th IEEE International Conference on Networks (ICON), pp. 171- 176, 2011.

[29] AlSa'deh Ahmad, Meinel Christoph, "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations", IEEE Security & Privacy, Vol.10, No.4, pp. 26-34, 2011.

[30] 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, pages 243-240.

[31] Youngsong Mun, Kyunghye Lee, Seonggeun Ryu and Teail Shin, "Using Return Routability for Authentication of Fast Handovers in Mobile IPv6", Computational Science and Its Applications (ICCSA 2007), published in Lecture Notes in Computer Science-4706, Volume 2, Published by Springer, ISBN:3-540-74475-4 978-3-540-74475-7, 2007, Page: 1052-1061.