The Research on Mobile IPv6 Security Features

Feng Xiaorong
Software Quality Testing Engineering Research Center,
China Electronic Product Reliability and Environmental
Testing Research Institute, Guangzhou, Guangdong,
510610, China
Email: fengxr@ceprei.com

Lin Jun, Jia Shizhun
Software Quality Testing Engineering Research Center,
China Electronic Product Reliability and Environmental
Testing Research Institute, Guangzhou, Guangdong,
510610, China

***Abstract*—along with the rapid progress and widely application of mobile network, mobile IPv6 security has become an important issue. By analyzing new features of mobile IPv6, the paper describes potential security threats hidden in protocol implementation, illustrates the principle of new security attacks and put forward corresponding preventive measures and technical solutions. New strategies including return to routing process, address validation and IPsec mechanism are proposed to satisfy mobile IPv6 security requirements.**

Keywords—IPv6 protocol; security attack; mobile terminal; information interception

I. INTRODUCTION

The rapid growth of intelligent mobile terminal users and fast development of Next Generation Network (NGN) have greatly promoted intelligent mobile terminal applications. With remarkable progress of its application, Internet protocol version 4 (IPv4) cannot satisfy special requirements of mobile Internet, such as security and network performance. At present, telecom operators gradually start to support Internet protocol version 6 (IPv6), including terminal, access and core network. Meanwhile, intelligent terminal manufactures also launch both software and hardware development supporting IPv6. Due to those factors mentioned above, mobile IPv6 application will become a trend inevitably.

In the Internet protocol family, IPv4 is mainly designed aiming at wired network mode. With limited number of IP address available for network distribution and insufficient support for network node mobility, IPv4 cannot satisfy mobile internet's development requirements. Based on original IP protocol, mobile IP protocol is proposed to support mobile nodes, which makes it realizable to access internet via various mobile devices under any circumstance. Mobile IP protocol is mainly designed to keep the continuity of communication between mobile nodes, without changing their IP address when connecting to other network access points. As a corporate body subordinate to IETF (Internet Engineering Task Force), mobile IP protocol group put forward IPv4 proposals in 1996[1], which have solved the reliability, security, scalability and media related problems of mobile Internet. Compared with mobile IPv4, mobile IPv6 combines with new features of IPv6 and makes further mobile nodes roaming in NGN more smoothly, thus the mobile network can be accessible at any time. Mobile IPv6 has more complete functions compared to IPv4, and it breaks several fundamental restrictions. It provides specific IP addresses for all mobile terminals and will eventually replace IPv4 using currently. Resolving the problem of IP address resource exhaustion as well as effective security supporting in network layer make it to be the dominant network protocol in NGN.

II. SECURITY FEATURES OF MOBILE IPV6

The security technology used in IPv6 is IPsec (IP Security). While the existing network of IPv4 could not be fully updated to support IPsec, IPv6 has realized all security requirements of IPsec [2]. Since many network attacks are carried out in network layer, the security service realized in IP layer can defend all kinds of network attacks more efficiently.

However, in terms of mobile IPv6, there are still many problems existing in protocol implementation [3]. As mobile node has to register current IP address to home agent as well as other communication nodes when moving away from home link, which would provide opportunities for network hacking in location registration process. In mobile Internet based on IPv6, most potential threats result from incorrect binding update information. Meanwhile, new technical characteristics defined in the agreement also have security vulnerabilities, and the support for nodes' mobility also has special effects for traditional network security protection.

III. SECURITY THREATS IN MOBILE IPV6 NEW FEATURES

In mobile IPv6 agreement, mobile node informs home agent and communication node of its current position through binding update information, which would make their data packet accessible to mobile node. The binding update information adapted in home agent or communication nodes create corresponding relations between home address and care-of-address for mobile node, which is stored in binding cache. Both home agent and communication nodes firstly have to check the binding cache so as to obtain the destination's care-of-address, and then, they send data packets to other nodes.

The key to binding update is the establishment of corresponding relations between home address and care-of-address for mobile node, which affects the home agent and communication nodes transmitting information to mobile node. Thus attackers make use of this process to induce security

978-1-4799-0156-2/13/$31.00 ©2013 IEEE

risks. Generally speaking, the attacks can be divided into four categories as follows:

A. Forged Binding update Attack

In normal circumstances, communication node would increase an item after receiving a binding update message, so as to map the mobile node's home address to care-of-address, and then, the data packets sent to mobile node would arrive at care-of-address [4]. However, if network attackers forge a certain binding update message and set a fake address for the care-of-address with other parts of the message unchanged, the data packets would be sent to forged mobile node. Therefore, the authentic mobile node would not be addressable.

Even the worse, the attackers probably use their personal address or other message receivers instead of fake address, so that the data packets would not be able to reach mobile node but are incepted by designated node. The authentic mobile node not only lose addressable feature but also make opportunities for attackers to obtain data packets which results in information lost.

Apart from this, some attackers send forged binding update message to multiple communication nodes, where the care-of-address is set as victim's home address. The data packets sent to mobile node by communication nodes would be re-directed to the victim, resulting in distributed reflection attack. In terms of the victim, since it receives plenty of data from communication nodes, it could not make normal response to communication requirements, which would induce denial of service attack.

The process of binding update information consumes certain calculation and storage resources. Thus network attackers make use of forged care-of-address to induce resource exhaustion, where the resources occupied by victims is not effectively released, and the overload system resource consumption causes denial of service attack. The forged binding update attack is shown in Figure 1:

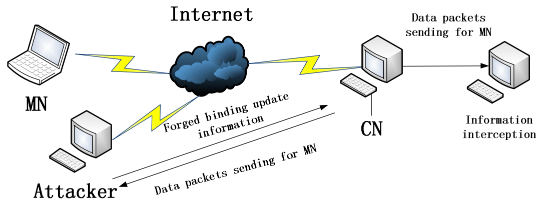


Fig1. The mechanism of forged binding update for information interception

B. Home Address Option Attack

In order to realize the addressable feature of mobile node when changing its location in communication links [5], mobile IPv6 agreement introduces some new headers and options in data packets and defines special treatment for those data packets. However, attackers also make use of new headers and options to induce hacking risks.

The home address option header defines 16 bytes to carry an IPv6 address, which belongs to the objective option header and is processed by destination node. The address defined in home agent address option represents original address, thus the destination node makes response in accordance with IPv6 address defined in those new home agent address option. Due to this feature, attackers could escape filter interface checking, make reflection attacks and intercept data message through new home address options.

Access router can filter data packets with wrong address in the topology of network through specific filter functions, which would prevent attacks in access network. However, the filter inspection would be avoided if attackers make use of home address option to fill the original address with correct topology structure and hide the authentic original address.

C. Routing Header Attack

In mobile IPv6, routing header of type 0 (RHT0) is defined to designate destination node for the data packet arrival. The next address illustrated in routing headers, would be the next destination node for subsequent data transmission. In this way, the transmission path arriving at destination node for designated data packets would be specified. Meanwhile, routing header of type 2 (RHT2) is defined to carry mobile node's home address, where mobile node could implement correct address registration and notify the corresponding relationships between home address and care-of-address to communication node, so that the routing optimization mechanism would be realized without relying on tunnel packet forwarding. The IPv6 address defined in RHT2 make data packets achieve authentic destination node. However, network attackers hide destination node address by use of address in RHT2 and implement address redirection and information interception.

D. Threats in Dynamic Mobile Prefix Discovery Mechanism

Mobile IPv6 agreements provide prefix discovery mechanism, where mobile node in foreign link could dynamically obtain information about home link's network topology and configuration modifications [6]. Thus the home address of mobile node can be modified all the time, which ensures its addressable feature.

Actually, in mobile prefix discovery mechanism, attackers at communication path between mobile node and home agent can obtain home link's network topology and configuration parameters information through eavesdropping technology. Meanwhile, they modify prefix data message in normal transmission which results in mobile node losing its addressable feature.

IV. PROTECTION STRATEGIES AGAINST SECURITY THREATS

A. Security Protection in Process of Registration

The key to against forged binding update is to provide authentication scheme for data packets receivers. Only after verifying the legitimacy of binding update, the receivers would allocate resources and make redirection for subsequent communication. In according to the application of scene and network deployment situation, security protection strategies for binding update information sent to home agent and communication nodes are as follows:

1) Communication node makes verification for the accessibility of mobile node's home address so as to ensure the mobile node's legitimacy;
2) Communication node makes verification for the accessibility of mobile node's care-of- address so as to ensure the care-of-address's validity;
3) The final binding update of mobile node would carry authentication information obtained through the above two steps.

Return to routing process is a typical application attributed to this type of solution, which is also a good solution recommended by mobile IPv6 [7]. Apart from this, IPsec (IP Security) strategy is used on the first two steps of the authentication information interaction for encryption transmission, so as to make attackers unable to obtain mobile node's authentication information sent by communication node. Therefore, the communication node would distinguish counterfeit binding updates efficiently. The diagram of return to routing process is shown in Figure 2:

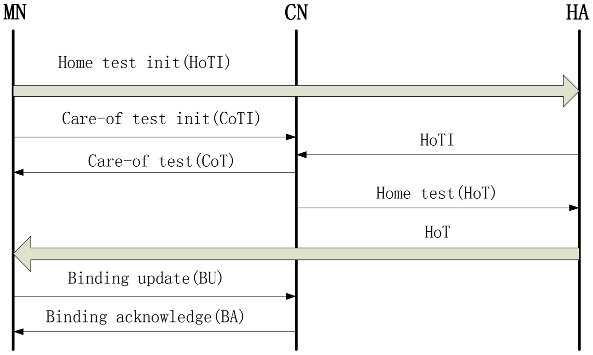


Fig2. Flow diagram of return to routing process

B. *Verification on Home Address Option and Routing Header*

The attack based on home address option aims to formulate or hide source address; therefore, strict verification for home address options is necessary to prevent illegal use of home address option. The validation process for home address option implemented by home agent is shown in Figure 3, and the process implemented by other communication nodes is in the same way.

RHT2 is defined to ensure that data packets could reach authentic destination node. The key to prevent routing header attack is to guarantee legality of routing header in data packet through mobile node's strict verification. The validation process is shown in Figure 4. The example to detect routing header attack without authentication in RHT2 is shown in Figure 5 and Figure 6, and the result of routing header attack after the validation process is shown in Figure 7.

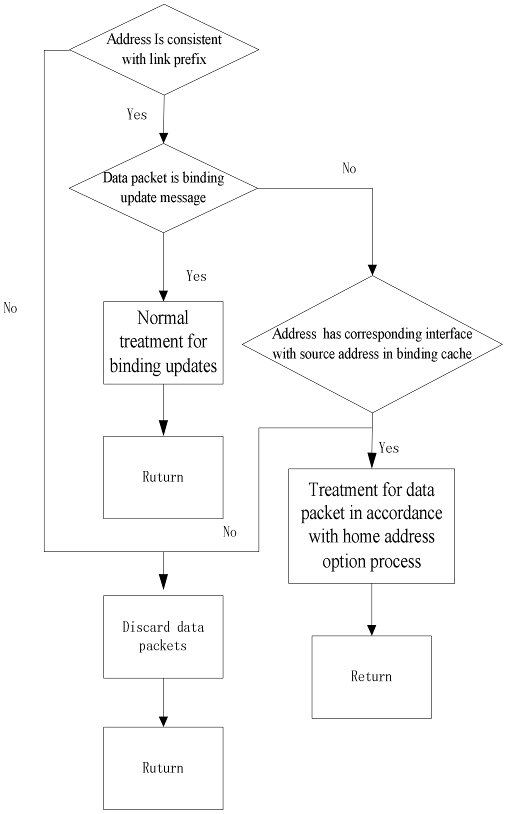

Address Is consistent with link prefix
Yes
No
Data packet is binding update message
No
Yes
Normal treatment for binding updates
Address has corresponding interface with source address in binding cache
Ruturn
Yes
No
Treatment for data packet in accordance with home address option process
Discard data packets
Return
Ruturn

Fig3. The validation process in RHT0

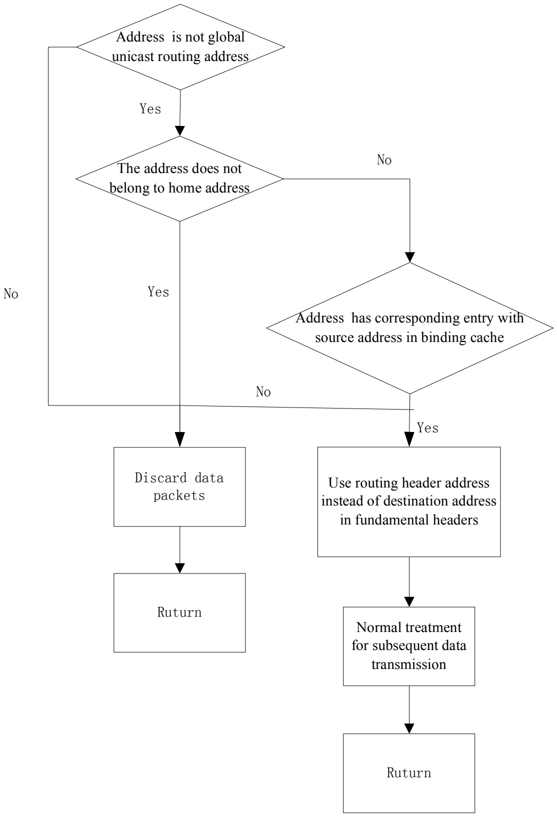
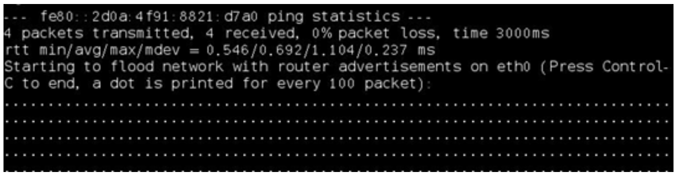
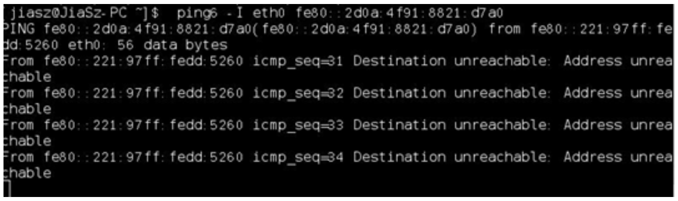

Address is not global unicast routing address
Yes
The address does not belong to home address
No
No
Yes
Address has corresponding entry with source address in binding cache
No
Yes
Discard data packets
Use routing header address instead of destination address in fundamental headers
Ruturn
Normal treatment for subsequent data transmission
Ruturn

Fig4. The validation process in RHT2



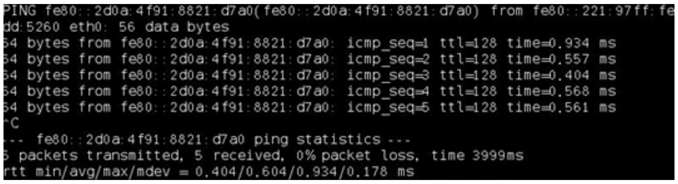
```
---  fe80::2d0a:4f91:8821:d7a0 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.546/0.692/1.104/0.237 ms
Starting to flood network with router advertisements on eth0 (Press Control-
C to end, a dot is printed for every 100 packet):
......................................................................
......................................................................
......................................................................
......................................................................
......................................................................
```

Fig5. Start the routing header attack without validation process in RHT2



```
[jiasz@JiaSz-PC ~]$  ping6 -I eth0 fe80::2d0a:4f91:8821:d7a0
PING fe80::2d0a:4f91:8821:d7a0(fe80::2d0a:4f91:8821:d7a0) from fe80::221:97ff:fe
dd:5260 eth0: 56 data bytes
From fe80::221:97ff:fedd:5260 icmp_seq=31 Destination unreachable: Address unrea
chable
From fe80::221:97ff:fedd:5260 icmp_seq=32 Destination unreachable: Address unrea
chable
From fe80::221:97ff:fedd:5260 icmp_seq=33 Destination unreachable: Address unrea
chable
From fe80::221:97ff:fedd:5260 icmp_seq=34 Destination unreachable: Address unrea
chable
```

Fig6. The result of routing header attack



```
PING fe80::2d0a:4f91:8821:d7a0(fe80::2d0a:4f91:8821:d7a0) from fe80::221:97ff:fe
dd:5260 eth0: 56 data bytes
64 bytes from fe80::2d0a:4f91:8821:d7a0: icmp_seq=1 ttl=128 time=0.934 ms
64 bytes from fe80::2d0a:4f91:8821:d7a0: icmp_seq=2 ttl=128 time=0.557 ms
64 bytes from fe80::2d0a:4f91:8821:d7a0: icmp_seq=3 ttl=128 time=0.404 ms
64 bytes from fe80::2d0a:4f91:8821:d7a0: icmp_seq=4 ttl=128 time=0.568 ms
64 bytes from fe80::2d0a:4f91:8821:d7a0: icmp_seq=5 ttl=128 time=0.561 ms
^C
---  fe80::2d0a:4f91:8821:d7a0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.404/0.604/0.934/0.178 ms
```

Fig7. The result of routing header attack after the validation process in RHT2

C. *IPsec Security Alliance*

During data transmission, IPsec security alliance [8] is applied to make identity authentication for data sources and protect data integrity, so as to ensure reliable implementations for mobile prefix discovery mechanism.

For one thing, mobile node has to make verification for notified prefix information, avoiding being cheated by error prefix data packet, which can be implemented through Authentication Header Protocol (AH) message validation. For another, encryption transmission mechanism should be used in mobile prefix message. This could be realized through Encapsulating Security Payload Protocol (ESP) encryption transmission, which ensures that the confidentiality of information is transmitted through full encryption of data packets, in order to prevent other users from snooping information by monitor.

V. CONCLUSION

New features defined in mobile IPv6 have potential security risks. Data packet header, routing options and implementation mechanisms tend to be security attack objects. The registration information which carries corresponding relationships between mobile node's home address and care-of-address is the key to mobile node's addressable feature, which is vulnerable to sorts of illegal attacks , thus security protection strategies would be necessary.

Return to routing process provides access for communication nodes to realize the ownership validation of mobile node's home address and care-of-address, which ensures the security of general registration. Validation on home address option and routing header is necessary to ensure about the source address's legality. Meanwhile IPsec mechanism is introduced to protect the data integrity in transmission so as to ensure about the mobile node's address feature.

ACKNOWLEDGMENT

The work was partially supported by the important and special project "Research on Mobile Intelligent Terminal Security Assessment Technology" sponsored by Ministry of National Science and Technique.

REFERENCES

[1] D Johnsom, C Perkins, J Arkko, Mobility Support in IPv6, RFC 3775. 2004

[2] Caicedo, Carlos E Joshi, B James etc. "IPv6 Security Challenges", [J]. IEEE Computer Society, Vol.42, No.2, pp. 36-42.2010

[3] Xianhua Jin, Dan Sui, "Study of IPv6 Security Technology", [C].The Proceeding of 2011 International Conference on Network and Electronic Engineering.2011

[4] 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.

[5] 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.

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

[7] Choudhary, Abdur Rahim, "Securing IPv6 Network Infrastructure: A New Security Model", IEEE International Conference on Technologies for Homeland Security (HST), pp. 500-506, 2010.

[8] Stamatios V.Kartalopoulos, " Differentiating Data Security and Network Security", [C]. Proceedings of the Symposium on Information and Network Security of ICC, 2008