Network Working Group
Internet-Draft
Expires: December 1, 2003

M. Bagnulo
A. Garcia-Martinez
I. Soto
UC3M
June 2, 2003

Preserving MIPv6 communications when the HoA becomes unreachable
draft-bagnulo-mobileip-unreachable-hoa-00

Status of this Memo

Copyright Notice

Abstract

This note proposes a modification to the MIPv6 specification in order to allow the preservation of established communications when the path between the MN and the CN through the HoA becomes unavailable. The proposed modification essentially consists on allowing the extension of BCE lifetime upon the reception of ICMP Destination Unreachable message as reply to a Binding Refresh Request (BRR) message.

1. Introduction

The MIPv6 [1] specification defines that Binding Cache Entries (BCE) that have been authorized using the Return Routability (RR) procedure have a maximum lifetime of MAX_RR_BINDING_LIFE (420 seconds). This means that the BCE linking a Home Address (HoA) and a Care-of Address (CoA) at the Correspondent Node (CN) will only remain valid for 7 minutes after the Binding Update (BU) reception. If this CoA is to be used to reach the HoA after this period, a new BU message binding the HoA and the CoA has to be sent. In order to be able to do this, the Mobile Node (MN) has to acquire new BU authorization data using the RR procedure, implying communication through both the CoA and the HoA. This implies that if the HoA becomes unreachable from the CN, the established communication will be interrupted because the BCE has expired, even if the path that is actually being used for the communication is still available. Summarizing, as currently defined, MIPv6 communication is vulnerable not only to outages along the communication path used to carry data packets, but also to outages along the path between the MN and the Home Agent (HA), and along the path between the HA and the CN. This behavior not only introduces additional points of failure in MIPv6 communications but it also limits the potential usage of MIPv6 to provide multi-homing support as described in [2].

This note proposes a modification to the MIPv6 specification in order to allow the preservation of established communications when the path between the MN and the CN through the HoA becomes unavailable. The proposed modification essentially consists on allowing the extension of BCE lifetime upon the reception of ICMP Destination Unreachable message as reply to a Binding Refresh Request (BRR) message.

2. Security Concerns that lead to reduced BCE lifetime.

In order to propose a modification to the defined behavior, we must first analyze the security concerns that lead to the current design.

BCE lifetime has been limited to a few minutes in order to limit the possibility of time shifting attacks, as it is presented in [3].

The goal of MIPv6 security is to avoid the introduction of new security hazards which are not present in non-MIPv6 enabled environments. In particular, the RR procedure limits the set of potential attackers to those who can intercept packets flowing between the CN and the HA. This procedure forces the attacker to be present somewhere along the path between the CN and the HA in order to acquire the valid authorization data needed to generate forged BU messages.

However, this mechanism by itself only imposes that the attacker has to be present on the path the time needed to intercept the messages that carry authorization information. Once that the attacker has intercepted the valid authorization information, he can leave his position along the path and still perform attacks using such information. These are called time shifting attacks, since an attacker that once was on-path intercepting packets can perform attacks in the future when he is no longer on the communication path.

The limitation of the BCE lifetime to a few minutes limits the effects of the following time shifting attack: the attacker placed along the communication path intercepts authorization information and generates a forged BU message. The attacker leaves the position but the attack continues since the traffic is still diverted to the CoA contained in the fake BU message. The effect of this attack is limited by reducing BCE lifetime in the CN to 7 minutes, imposing the generation of a new BU message in order to restore the BCE. Since the attacker is no longer along the communication path, he will not be able to generate new BU messages.

3. Proposed modifications to the MIPv6 specification

Currently time shifting attacks are prevented by imposing periodical message exchange which imply that the attacker has to be present along the path between the CN and the MN's HoA in order to continue with the attack. So, the currently available mechanism assumes that an attack is being perpetrated when no information can be exchanged with the other end through the HoA. However, it is not really necessary to perform a message exchange with the MN to prevent a time shifting attack. The only thing that is really needed is a mechanism that requires the presence of the attacker along the path between the CN and the MN's HoA in order to continue with the attack. This can be achieved through a message exchange with any device along the path which does not has to be the communicating end-points. This note proposes the exchange of messages between the CN and the first router with no route to the final destination address as a time shifting attack prevention mechanism when the HoA is unreachable from the CN.

3.1 Proposed mechanism

3.1.1 Correspondent Node Part

When the remaining lifetime of an existent BCE reaches 32 seconds, the CN sends a Binding Refresh Request (BRR) to the MN's HoA for this binding. The timeout for this request is set to 1 second. If no response is obtained within this interval, the CN retransmits the BRR until a response is received or the BCE lifetime expires.

The BRR message contains a Cookie Mobility option as defined in section 3.2. This option contains a 64-bit randomly generated cookie which will be copied to the response packets in order to verify that the replying party has received (or intercepted) the BRR.

If the MN is reachable through the HoA, and it is interested in preserving the BCE valid, it will send a BU message, extending the BCE lifetime.

However, if an outage has occurred along the path between the CN and the MN's HoA, an ICMP Destination Unreachable message containing a No Route to Destination Code will be generated by a router along the path according to [4]. The ICMP message contains the ICMP header and it will will be completed with as much of the invoking packet as it will fit within the MTU defined for IPv6 [5], which is 1280 bytes. This means that the complete BRR message, including the newly defined cookie option will be included within the ICMP message.

When the CN receives an ICMP Destination Unreachable message containing a No Route to Destination Code, it verifies that the ICMP

message was generated as a reply to the BRR. It does so by verifying that the packet included in the ICMP message is a BRR message and that the cookie included in the Cookie Mobility Option matches with the one included in the initial BRR message. If the verification succeeds, the CN detects that an outage has occurred and extends the BCE lifetime for 180 seconds, preserving the established communication through the CoA. After 150 seconds, a new BRR message will be sent.

The BCE lifetime can only be renewed 60 times, limiting to 3 hours the maximum time that an BCE entry can be valid without performing the RR procedure.

3.1.2 Mobile Node Part

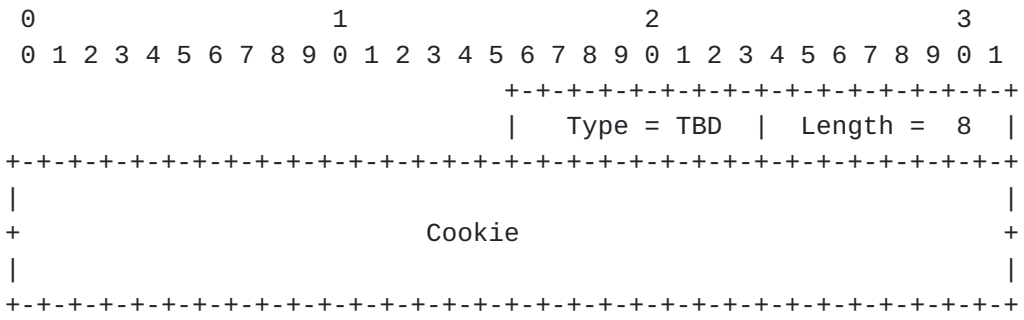
A similar mechanism is to be implemented in the MN in order to preserve the state needed in the MN to maintain the established communication, so that the MN continues to send packets directly to the CN without using the HA. Such state is stored in the Binding Update List (BUL) within the MN and it has a limited lifetime, imposing its periodical refresh. So when a BUL entry is about to expire, the RR procedure is to be performed so that the authorization information needed to send a BU message is acquired. The RR procedure consists on the exchange of the CoTI/CoT messages directly between the CN and the MN and the exchange of the HoTI/HoT messages through the HA. If the path between the CN and the MN's HoA is working properly, the RR procedure will be completed successfully and a new BU message will be issued, and the lifetime of the BUL entry corresponding to that CN will be extended. If the path between the CN and the MN's HoA is not working, the RR procedure will not be completed, preventing the generation of the BU message, implying that the BUL entry corresponding to that CN will expire. This means that forthcoming packets will be sent from the MN to the CN through the HA and since there is no path available, the communication will fail.

It is proposed that the BUL lifetime is extended upon the reception of an ICMP Destination Unreachable message containing a No Route to Destination Code as a reply to a HoTI message issued by the MN. The resulting behavior is that when a BUL entry is about to expire, the MN will initiate the RR procedure sending a HoTI and a CoTI message. If there is no route available between the CN and the MN through the HA, an ICMP Destination Unreachable message containing a No Route to Destination Code is be sent back to the MN. Then, when the MN receives such message, it verifies that the ICMP message was generated as a reply to the HoTI message. It does so by verifying that the packet included in the ICMP message is a HoTI message and that the cookie included in the Home Init Cookie field matches with the one included in the initial HoTI message. If the verification

succeeds, the MN detects that an outage has occurred and extends the BUL lifetime for a period equal to the initial value of the lifetime (contained in the BUL entry), preserving the established communication.

3.2 Cookie Mobility Option

The Cookie option has the following format:



This Mobility Option contains a 64 bit long randomly generated cookie.

4. Security Considerations

This note proposes changes to MIPv6 security. The reader is referred to section 2 for the risks that the modified security features prevent and to section 3 for an analysis of the proposed changes.

5. Acknowledgments

Thanks to Pekka Nikander for suggesting a more general problem for the solution proposed in this document and also for providing many constructive comments.

References

[1] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", Internet Draft, Work in progress draft-ietf-mobileip-ipv6-21.txt, May 2002.

[2] Bagnulo, M., Garcia-Martinez, A. and I. Soto, "Application of the MIPv6 protocol to the multi-homing problem", Internet Draft, Work in progress draft-bagnulo-multi6-mnm-00, February 2003.

[3] Nikander, P., Aura, T., Arkko, J. and G. Montenegro, "Mobile IP version 6 (MIPv6) Route Optimization Security Design Background", Internet Draft, Work in progress draft-nikander-mobileip-v6-ro-sec-00, March 2003.

[4] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)Specification", RFC 2463, December 1998.

[5] Hinden, R. and S. Deering, "Internet Protocol, version 6(IPv6) Specification", RFC 2460, December 1998.

Authors' Addresses

Marcelo Bagnulo
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: 34 91 6249500
EMail: marcelo@it.uc3m.es
URI: http://www.it.uc3m.es/marcelo

Alberto Garcia-Martinez
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: 34 91 6249500
EMail: alberto@it.uc3m.es
URI: http://www.it.uc3m.es/alberto

Ignacio Soto
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: 34 91 6249500
EMail: isoto@it.uc3m.es
URI: http://www.it.uc3m.es/isoto

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.