Network Working Group
Internet-Draft
Expires: December 25, 2005

F. Dupont
Point6

June 23, 2005

A note about 3rd party bombing in Mobile IPv6
draft-dupont-mipv6-3bombing-02.txt

Status of this Memo

Copyright Notice

Abstract

Mobile IPv6 introduces some new kinds of reflection attacks, as known as 3rd party bombing. This memo analyses these attacks and makes some recommendations: the goal is to avoid anything, including in new optimized mechanisms, which can make the life of bad guys easier.

1. Introduction

The standard reflection attack is based on the "bombing" of a 3rd party, the victim, by a reflector:

- the attacker A sends requests to the reflector R using the address of the victim V as the source address of requests
- the reflector R sends (large) answers to V.

In the mobile IPv6 [RFC3775] context, the attacker is a mobile node, the reflector a correspondent node (a common one or the home agent).

There are two basic defenses against the reflection attack:

- ingress filtering [BCP38] (improved in [BCP84]), i.e., checking that source addresses are topologically correct
- all protocols which needs some kind of positive feedback from peers, as TCP or RTP/RTCP.

As a correspondent node sees two addresses (a transient care-of address and the home address) per mobile node, it is clear that mobile IPv6 can add new opportunities to reflection attacks...

2. Analysis

There are three different kinds of reflection attacks using mobile IPv6 mechanisms, one for each mode of operation: triangular routing, bidirectional tunneling and routing optimization.

Note that the attack is always from the mobile node itself, i.e., no intermediate node can successfully modify packets in transit to launch an attack as in the transient pseudo-nat attack [ID.transient-pseudonat].

At the opposite, a local / visited network access control with an AAA architecture [ID.aaa-mipv6-requirements] or an equivalent can give some real guarantees about a care-of address, i.e., something better than just trusting mobile nodes.

The basic argument of this document is the ingress filtering is the right defense against reflection attacks and similar threats like address stealing and network bombing.

2.1 Triangular routing

In this case the mobile node sends packets carrying in the home address option a fake home address. The correspondent node sends back traffic to this home address. In order to avoid a very dangerous attack (bombing traffic with no trace of the attacker) the mobile IPv6 specifications [RFC3775] mandates the verification of home address options:

- when a packet with a home address option matches a binding cache entry it is accepted, but routing optimization is active: this case will be analyzed further.

- when a proper IPsec security association exists, but in this case the home address is proven.

So there is no reflection attack issue with triangular routing.

2.2 Bidirectional tunneling

This mode is the basic one: all traffic from or to the mobile node goes through a bidirectional tunnel between the mobile node and its home agent.

In order to launch a reflection attack the mobile node has to put a fake care-of address in binding updates sent to its home agent (home registrations). The home agent does not perform a routing routability check, i.e., it does not check if the mobile node is really reachable at its current care-of address. This point was discussed (issue 34 [ISSUE34]) by the mobileip working group which decided:

"The above mechanisms do not show that the care-of address given in the Binding Update is correct. This opens the possibility for Denial-of-Service attacks against third parties. However, since the mobile node and home agent have a security association, the home agent can always identify an ill-behaving mobile node. This allows the home agent operator to discontinue the mobile node's service, and possibly take further actions based on the business relationship with the mobile node's owner."

Note that the registration of a fake care-of address diverts all the traffic to the mobile node via the home agent and at least 40 octets is added to each packet, so for an attacker this attack is more effective than the next one.

2.3 Routing optimization

The last mode is the routing optimization: binding updates sent by the mobile node create or update binding cache entries on the correspondent node. A routing header of type 2 is added to each packet to the mobile node with its home address, so the extra information uses 24 octets and reveals the home address.

The reflection attack in the routing optimization case uses fake care-of addresses in binding updates sent from the mobile node to the correspondent node. Usually the care-of address is in the source address field of the IPv6 header but it can be, with a different value, in an alternate care-of address option too. So the only security issue can come from this option because a fake care-of address in the IPv6 header is not a different case than a fake source address, i.e., the routing optimization does not modify the basic

reflection attack.

When the return routability procedure is used with an alternate care-of address, it is applied to the right address (issue 5 [ISSUE5]). When some other mechanisms is used, usually a longer term one, either a return routability check must be performed, using a third packet (aka a hand-shake) repeating a cookie from the binding acknowledgment [ID.mipv6-rrcookie] or binding updates with different care-of addresses in the IPv6 header and in the alternate care-of address option must be refused.

2.4 Home network bombing

The last attack uses a fake home address and simulates a "return to the home". Pending traffic is redirected to the the home address and can flood the home network. Further traffic has to be sent from the fake home address so this is the standard reflection attack.

3. Current attacks using fake source addresses

Reflection attacks are only one kind of attacks based on the use of fake source addresses. Current distributed denials of service (DDoS) use a large number of compromised nodes (BOTs [Botnets]) and do not take advantage of possible amplification by reflection, and this fact should not change in the future.

4. Conclusion

We recommend that alternative ways to build security associations to protect signaling between mobile and correspondent nodes do not blindly accept "hidden" care-of addresses. As the goal of these ways is to be more efficient than the return routability procedure, IMHO their specifications must either forbid alternate care-of address options which carry different addresses than source addresses of IPv6 headers or must provide an explicit counter-measure (like [ID.mipv6-rrcookie]).

We recommend to avoid unnecessary return routability checks because:

- return routability does not give better assurance than ingress filtering: both check if the source is on the returning path.
- return routability is an active device which has a cost in extra messages and delays, ingress filtering is a passive device which can be done at any line speed with hardware support.
- if ingress filtering is not applied, the network is open to any attacks based on fake source addresses, including current DDoS which are (as we get the proof everyday) far more then enough to kill a target attached as any speed to the network.

5. Security Considerations

This goal of this document is to verify that mobile IPv6 mechanisms cannot be misused to make reflection attacks easier. As the return routability procedure [ID.ro-sec] is not considered by many people as very safe or efficient, some new ways to build security associations to protect mobile IPv6 signaling are likely to appear [ID.ro-enhance], so they should be carefully designed...

6. Acknowledgments

Some persons stressed Wassim Haddad to add some defense against reflection attacks to his optimized mobile IPv6 [ID.mipv6-omipv6] when this is both unnecessary and of course against the idea of optimization.

Pekka Savola raised our attention about [BCP84] which improved ingress filtering in multi-homed environments.

7. References

7.1 Normative References

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

7.2 Informative References

[BCP38] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, BCP 38, May 2000.

[BCP84] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", RFC 3704, BCP 84, March 2004.

[Botnets] Kristoff, J., "Presentation at NANOG 32 on botnets", October 2004, <http://www.nanog.org/mtg-0410/kristoff.html>.

[ID.aaa-mipv6-requirements] Faccin, S., Le, F., Patil, B., Perkins, C., Dupont, F., Laurent-Maknavicius, M., and J. Bournelle, "Mobile IPv6 Authentication, Authorization, and Accounting Requirements", draft-le-aaa-mipv6-requirements-03.txt (work in progress), February 2004.

[ID.mipv6-omipv6] Haddad, W., Dupont, F., Madour, L., Krishnan, S., and S.

Park, "Optimizing Mobile IPv6 (OMIPv6)", draft-haddad-mipv6-omipv6-01.txt (work in progress), February 2004.

[ID.mipv6-rrcookie]
Dupont, F. and J-M. Combes, "Care-of Address Test for MIPv6 using a State Cookie", draft-dupont-mipv6-rrcookie-01.txt (work in progress), June 2005.

[ID.ro-enhance]
Arkko, J. and C. Vogt, "A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization", draft-irtf-mobopts-ro-enhancements-00.txt (work in progress), January 2005.

[ID.ro-sec]
Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP version 6 Route Optimization Security Design Background", draft-ietf-mip6-ro-sec-03.txt (work in progress), June 2005.

[ID.transient-pseudonat]
Dupont, F. and J-J. Bernard, "Transient pseudo-NAT attacks or how NATs are even more evil than you believed", draft-dupont-transient-pseudonat-04.txt (work in progress), June 2004.

[ISSUE34] Yegin, A., Arkko, J., and F. Dupont, "MIPv6 issue 34: CoA test also for home registrations? (Rejected, included in draft 18)", May 2004, <http://users.piuha.net/jarkko/publications/mipv6/issues/issue34.txt>.

[ISSUE5] Arkko, J., Ed., "MIPv6 issue 5: Alternative-CoA usage rules (Adopted, included in draft 17)", May 2004, <http://users.piuha.net/jarkko/publications/mipv6/issues/issue5.txt>.

Author's Address

Francis Dupont
Point6
c/o GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: Francis.Dupont@enst-bretagne.fr

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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