Internet Engineering Task Force
INTERNET DRAFT
Expires in July 2002

Francis Dupont
ENST Bretagne
Claude Castelluccia
INRIA

January 2002

IPv6 Network Ingress Filtering

<draft-dupont-ipv6-ingress-filtering-00.txt>

Status of this Memo

Abstract

This document describes how network ingress filtering should be done for the IPv6 protocol, including with mobile IPv6.

Ingress filtering is a standard reply to Distributed Denial of Service (DDoS) using forged source addresses. A priori ingress filtering can be done anywhere but is most efficient when it is done by border routers of the source site. This can be considered as a form of "responsible use of the network".

Mobile IPv6 amplifies the DDoS threat with the home address option: this can be used in order to add an indirection level in DDoS attacks and to foul simple ingress filtering. The proposed reply is a better ingress filtering. This document explains how to improve basic anti-spoofing filtering too.

1. Introduction

In a DDoS attack a large number of compromised nodes "As" send a lot of packets to a target "T" using forged source addresses [1]. The reply is to verify the validity of source addresses, i.e. to do network ingress filtering and/or to try to find the real sources like with itrace [2].

Ingress filtering can be done inside a backbone at aggregation points, using unicast Reverse Path Forwarding (uRPF) check, i.e. verifying that the incoming traffic interface and the route to the source address match. This has some issue with multi-homing, stressed by IPv6, even if contrary to a common myth uRPF can work with asymmetrical routing [3].

Another (better) choice is to implement ingress filtering in Internet connectivity border router, i.e. to put a fire-wall which filters traffic from inside the site to the Internet. This is not so uncommon: this kind of filters is heavily used (or should be heavily used) when Internet access is provided to an unskilled or untrusted community (cybercafes, student rooms, ...). One can consider this as a form of "responsible use of the network" enforcement.

Mobile IPv6 [4] introduces a new issue: the home address option which contains an alternate source address (a mobile node sends packets with a care-of address as the source address in the IPv6 header and with the home address in the home address option). When the home address option is processed by the node receiving a packet with it, the alternate source address replaces the original source address, i.e. the traffic seems to come from the alternate source address but but the source address seen by simple ingress filtering devices is topologically correct.

A node blindly processing home address options can be used as a reflector, i.e. in a iDDoS attack some nodes "As" send a lot of packets with their own source addresses and a home address option with the address of the target "T" to reflectors "Rs". Reflectors "Rs" send replies to "T". This is a flood of replies, less dangerous by far enough if the purpose is to overload "T" or its infrastructure. The advantage of bad guys is the traffic from "Rs" to "T" does not mention "As": trace back is far more difficult.

The threat is against ingress filtering: simple ingress filtering devices check only the source address in the IPv6 header, not the alternate source address in the home address option. So the basic solution is to verify both addresses are legitimate, i.e. to know the "binding" between the two addresses.

The remainder of the document will essentially explain how to use this knowledge. Note the home address option is a degenerate case of tunneling where inner and outer destination addresses are the same [5]. The same threat (and the same solution) exists with tunneling but, by simplicity, this document deals only with in the current mobile IPv6 context.

2. Correspondent Nodes

The first solution is to use the knowledge of bindings in correspondent nodes: when a packet is received with a home address option, it is checked against the binding cache. If it does not match, it is declared invalid.

This solution is too drastic and leaves only two modes to mobile IPv6: bidirectional tunnel between the mobile node and its home agent, or routing optimization, i.e. two way direct communication between the mobile node and its correspondent, using home address options and routing headers. The asymmetrical medium possibility is no more available.

Of course, this cannot work without bindings, i.e. this solution is not applicable to other uses of home address options than mobile IPv6.

Our opinion is that binding cache entry check should be used only as a sanity check.

3. Smart Ingress Filtering

The second solution is to use better ingress filtering in the access network: fire-walls between the access network know active bindings and check outgoing traffic against them. If it does not match the action is the same than with forged source addresses.

The main issue with this solution is how to get the knowledge of bindings. The proposal is to improve the network access control: as a node inside the site should not be allowed to use an unauthorized source address, a mobile node inside the site has to declare in addition via the network access control system its home address(es), or filters will not be "opened" for its home address options.

Mobile IPv6 and AAA drafts [6b, 7] have already this feature: the local/visited AAA server has the knowledge of care-of and home address(es), home agent address, ... More, home related informations are certified by the home/remote AAA server: smart ingress filtering doesn't rely on AAA infrastructure availability but an AAA infrastructure shall provide many new/extra features.

This solution has two drawbacks: fire-walls enforcing it are more complex, for instance they have to manage some state (even if the state is the network access control system too). This solution relies in an advanced network access control too, but one may say that without a good network access control an Internet access provider is only a danger for everybody, i.e. this is more a "how to enforce a Best Current Practice" than a technical issue.

4. Other Threats

4.1 Smart Anti-Spoofing Filtering

A common and very useful filtering rule is to forbid traffic from the outside using an inside address as source. Of course, this has to be extended to home address options.

The only valid case of an inside address in a home address option is for a mobile node which belongs to the site, i.e. its home site is the site. So the knowledge of special binding cases, home registrations, are enough. In general, one can assume the possible home addresses and home agent addresses are known, this provides a basic protection against random home address option or binding updates.

The needed knowledge of home registrations can be gained from binding update/binding acknowledge exchanges or better from home agent collaboration, for instance through the remote network access control system (the home/remote AAA server of mobile IPv6 and AAA drafts [6b, 7]), or (second example from a Michael Thomas' proposal) by reflecting the binding update/binding acknowledge exchange (i.e. home agents send the contents of the two packets of home registrations to the border routers of the home domain.

This has the same drawbacks than for the smart ingress filtering but the home agent function is a more advanced feature than Internet access, so the required extra control should be easier to enforce (for instance the part of the site where there may not be a home agent is easy to protect by simply applying the anti-spoofing rule to home address options).

4.2 Rogue Routing Headers

Even if nodes should deal with rogue routing headers with a proper policy, especially hosts (there is consensus about sound policies but there are not *yet* documented in a (partial) requirements for IPv6 hosts document), with binding knowledge a fire-wall can easily detect rogue routing headers.

The filtering rule to apply is exactly the symmetrical rule than for home address options. Of course, all other things are the same. This is not crucial but to know when one is under attack is in general useful so this should be done (belt and braces too).

4.3 Rogue Tunneling

The current mobile IPv6 uses only tunneling between the mobile node and the home agent. If the inner IPv6 header is not hidden, filtering rules similar to home address option and routing header rules should be applied with the constraint that the peer of the mobile node is the home agent.

If the inner IPv6 header is hidden (by ESP for instance), this should be authorized according to security policy rules (this can be an issue because a protected tunnel with the outside may infringe the Bell-LaPadula write rule [8]). The fact that the tunnel is for mobile IPv6 if and only if peers are the mobile node and its home agent should be used, for instance one can deny the use of tunnels by inside nodes which have not negotiated mobility stuff.

5. Security Considerations

Today the best rely to Distributed Denial of Service attacks is the network ingress filtering. Ingress filtering can be a bit harder for IPv6 but mobile IPv6 introduces a new threat because of one of its basic feature, the home address option.

This document argues as the home address option defeats simple ingress filtering, the solution is to use better ingress filtering which can be applied if the network access control provides the knowledge of bindings to fire-walls between the access network and the Internet.

6. Acknowledgments

This problem was discussed inside the MobiSecV6 project many years ago (the MobiSecV6 project joined mobility and security, especially fire-wall, people). As ingress filtering is not really enforced the threat was considered as minor (i.e. we knew a good reply) but the security requirements of mobile IPv6 were recently revisited, including this issue, and too drastic IMHO solutions proposed [9].

We apologized because our intention was to publish this document near one year ago. Unfortunately we spent to much time on warm mailing list discussion and we let fear, uncertainty and doubt settle when we knew by our concrete experience that secure mobile IPv6 is possible.

Thanks to (from North to South), Pekka Nikander, Pekka Savola, Jari Arkko, Stanislav Shaluno, Michael Thomas, ...

7. Normative References

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

8. Informative References

[2] S. Bellovin, M. Leech, T. Taylor, "ICMP Traceback Messages", draft-ietf-itrace-01.txt, October 2001.

[3] Cisco, "Unicast Reverse Path Forwarding (uRPF) Enhancements for the ISP-ISP Edge", http://www.cisco.com/public/cons/isp/documents/uRPF_Enhancement.pdf, February 2001.

[4] D. Johnson, C. Perkins, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-15.txt, July 2001.

[5] S. Deering, B. Zill, "Redundant Address Deletion when Encapsulating IPv6 in IPv6", draft-deering-ipv6-encap-addr-deletion-00.txt, November 2001.

[6] F. Dupont, M. Laurent-Maknavicius, J. Bournelle, "AAA for mobile IPv6", draft-dupont-mipv6-aaa-01.txt, November 2001.

[7] S. Faccin, F. Le, B. Patil, C. Perkins, "Diameter Mobile IPv6 Application", draft-le-aaa-diameter-mobileipv6-01.txt, November 2001.

[8] D. Bell, L. LaPadula, "Secure Computer System: Unified Exposition and Multics Interpretation", MTR-2997 rev. 1, March 1976.

[9] P. Savola, "Security of IPv6 Routing Header and Home Address Options", draft-savola-ipv6-rh-ha-security-01.txt, November 2001.

9. Authors' Addresses

Francis Dupont
ENST Bretagne
Campus de Rennes
2, rue de la Chataigneraie
BP 78
35512 Cesson-Sevigne Cedex
FRANCE
Fax: +33 2 99 12 70 30
EMail: Francis.Dupont@enst-bretagne.fr

Claude Castelluccia
INRIA Rhone-Alpes
655, avenue de l'Europe
38330 Montbonnot Saint-Martin
FRANCE
Fax: +33 4 76 61 52 52
EMail: claude.castelluccia@inria.fr