Note about Routing Header Processing on IPv6 Hosts
draft-savola-ipv6-rh-hosts-00.txt

Abstract

[IPV6] specifies routing header processing for nodes. The text is sufficiently ambiguous where the behaviour of hosts is concerned, and can be perceived as a security threat. This draft clarifies the issue by referring to IPv4 Host Requirements document and requiring hosts must not, by default, forward routing headers outside of the node.
1. Issue with Routing Header Processing

[IPV6] specifies routing header processing for nodes. The text is sufficiently ambiguous, especially the 3rd paragraph on page 13, to make one believe that routing header forwarding should be enabled on all nodes (including hosts); a few implementations are known to have interpreted the specification this way.

For clarification, it should be noted that IPv4 Host Requirements [HOSTREQ], especially section 3.3.5 should be interpreted to apply here where appropriate; the interpretation of [IPV6] is that every node must be able to process routing headers, but not every node needs to have that processing enabled.

See Appendix A for an example set of IPv6 requirements for routing header forwarding.

2. Security Considerations

This draft and [RHHASEC] discuss security considerations of processing packets with a routing header.

[HOSTREQ] permits implementations to perform "local source-routing", that is, forwarding routing header out on the same interface it was received from, without restrictions even on hosts. This is a security threat, as pointed out in [RHHASEC], and it is recommended that IPv6 implementations will not do that.

Moreover, as [RHHASEC] points out, forwarding routing headers inside the same node has residual security threats as well: consider a host with two interfaces that belong to different security zones. These kind of nodes are often "security gateways", though, and some may see this as an acceptable risk.

3. Acknowledgements

Francis Dupont for long and colourful discussion on the RFC2460 interpretation, Vlad Yasevich for pointing out an RFC2460 forwarding definition and Erik Nordmark for refining the rules. The issue was raised primarily due to Mobile IPv6 concerns.
4. References


Author’s Address

Pekka Savola
CSC/FUNET
Espoo, Finland
EMail: psavola@funet.fi

A. An example set of rules for IPv6 RH forwarding for hosts

Here, abbreviation ‘RH packet’ is used to mean a packet with routing header which has segments left > 0 and would be processed at the node (that is, destination address is an address of the node).

A host MUST NOT by default forward RH packets out of the node. This option MAY be configurable, but MUST default to disabled.

A host MAY restrict forwarding RH packets in the node as well, e.g. by disabling all routing header processing by default. [Note: the author believes this should be a SHOULD]

A host MAY provide some mechanisms of allowing acceptable routing header use, for example, allow RH where the address-to-be-changed and source address are the same, or allow forwarding out of the same interface the packet was received from.

A host which forwards source routed packets MUST behave the same way as a router doing this e.g. in terms of sending ICMP error messages.