Internet Draft
draft-rja-ilnp-nonce-11.txt
Expires: 27 JAN 2012
Category: Experimental

RJ Atkinson
Consultant

27 July 2011

ILNP Nonce Destination Option
draft-rja-ilnp-nonce-11.txt

Status of this Memo

Distribution of this memo is unlimited.

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Abstract

This document describes an experimental Nonce Destination Option that is part of the Identifier-Locator Network Protocol (ILNP). This option is used with the ILNP variant that is based upon IPv6. This is a product of the IRTF Routing RG.

Table of Contents

1. Introduction

Some in the research and development community are examining different approaches to evolving the Internet Architecture. Several different classes of evolution are being considered. One class is often called "Map and Encapsulate", where traffic would be mapped and then tunnelled through the inter-domain core of the Internet. Another class being considered is sometimes known as "Identifier/Locator Split".[GSE] [8+8]

This document is part of a proposal that is in the latter class of evolutionary approaches. This particular approach, the Identifier-Locator Network Protocol (ILNP), described in this document and in related Internet-Drafts, is based upon IPv6. [ILNP-Intro] [ILNP-DNS] [ILNP-ICMP] [RFC 2460]

The Nonce option for the IPv6 Destination Options Header that is described in this document provides two functions. First, it provides protection against off-path attacks for packets when an Identifier/Locator split is in use. Second, it provides a signal during initial IP session creation that the Identifier/ Locator Split operating mode is proposed for use with this session. This last function is particularly important for ensuring that the new Identifier/Locator Split operating mode is both incrementally deployable and backwards compatible with IPv6. Consequently, this option must not be used except by a node operating in the I/L Split (ILNP) mode.

Further, each Nonce value is unidirectional. Since packets often travel asymmetric paths between two correspondents, having separate Nonces for each direction limits the number of on-path nodes that can easily learn a session's nonce. So a typical TCP session will have 2 different nonce values in use: one nonce is used from Local Node to the Correspondent Node and a different nonce is used from the Correspondent Node to the Local Node.

Before reading this draft, readers should read the related Internet-Draft titled "ILNP Concept of Operations", as that document will help the reader understand the overall context for this option.[ILNP-Intro]

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. [RFC 2119]

2. Syntax

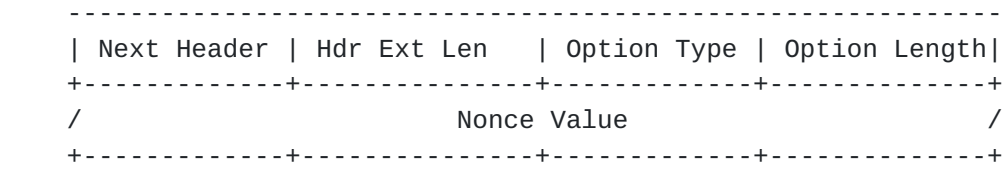
The Nonce Option is carried within an IPv6 Destination Option Header. Section 4 of [RFC 2460] provides much more information on the various options and optional headers used with IPv6. Note well that the IP Authentication Header is neither an IPv6 Destination Option nor an IPv6 Hop-by-Hop Option because it is instead its own header type.[RFC 4302]

More than one option might be inside the IPv6 Destination Option Header, however at most 1 Nonce Option exists in a given IPv6 packet.

A system that receives a packet containing more than one Nonce option SHOULD discard the packet as "Authentication Failed" (instead of passing the packet up to the appropriate transport-layer protocol or to ICMP) and log the event, including the Source Locator, Source Identifier, Destination Locator, Destination Identifier, upper-layer protocol (e.g. OSPF, TCP, UDP) if any, and transport-layer port numbers (if any), as a security fault in accordance with local logging policies.

As of this writing, IPv6 Destination Option Headers, and the options carried by such headers, are extremely uncommon in the deployed Internet. So, it is expected that this Nonce Option commonly would be the only IPv6 Destination Option present in a given IPv6 packet.

In the diagram below, we show not only the Nonce Option, but also the IPv6 Destination Option Header that carries the Nonce Option.



Next Header: 8-bit selector. Identifies the type of header immediately following the Destination Options header. Uses the same values as the IPv4 Protocol field [RFC 1700 et seq.].

Hdr Ext Len: 8-bit unsigned integer. Length of the Destination Options header in 8-octet units, not including the first 8 octets.

Option Type: This contains the value XXX, which is used

to indicate the start of the Nonce Option.

Option Length: This indicates the length in 8-bit octets of the Nonce Value field of the Nonce Option. This value must be selected so that the enveloping IPv6 Destination Option complies with the IPv6 header alignment rules. Common values are 4 (when the Nonce Value is 32-bits), and 12 (when the Nonce value is 96-bits).

Nonce Value: An unpredictable cryptographically random value used to prevent off-path attacks on an ILNP session. [RFC 4086] This field has variable length, with the length indicated by the Option Length field preceding it. Note that the overall IPv6 IPv6 Destination Option must comply with IPv6 header alignment rules. Implementations must support sending and receiving 32-bit and 96-bit Nonce values.

3. Transport Protocol Effects

When the initial packet(s) of an IPv6 session contain this Nonce Destination Option, the Identifier/Locator Split operating mode is in use for that IP session.

When an IPv6 session is in the Identifier/Locator Split operating mode, the transport-layer pseudo-header calculations zero the high-order 64-bits ("Locator" or "Routing Prefix") of each IPv6 address. This has the effect that the transport-layer is no longer aware of the topological network location of either node in the session.

The preceding rule applies not only to unicast sessions, but also to multicast or anycast sessions when the Identifier/Locator Split operating mode is in use.

4. Location Changes

When a node has an unexpected change in its Locator set that causes all previously valid Locators to become invalid, the node must send an ICMP Locator Update message (containing the Nonce Option with the appropriate nonce value) to each of its correspondents.

In the deployed Internet, packets sometimes arrive at a destination out of order. A receiving node MUST drop a packet

arriving from a correspondent if the Source Locator of the received packet is not in the receiving node's ILNP Correspondent Cache's Set of Correspondent Locator(s) UNLESS that packet contains a Nonce Option with the appropriate nonce value for that Source Identifier and Destination Identifier pair. This is done to reduce the risk of session hijacking or session interference attacks.

Hence, the node that unexpectedly had all previously valid Locators become invalid must include the Nonce Option with the appropriate nonce value in all packets (data or otherwise) to all correspondents for at least 3 round-trip times for each correspondent. (NB: An implementation need not actually calculate RTT values; it could just use a fixed timer with a time long enough to cover the longest RTT path, such as 1 minute.) This 'gratuitous authentication' ensures that the correspondent can authenticate any received packet, even if the ICMP Locator Update control message arrives and is processed AFTER some other packet using the new Source Locator(s). If a session is using IP Security, then, of course, IP Security should continue to be used in this case. Because IP Security for ILNP binds only to the Identifiers, and not to the Locators in the packet, changes in Locator value have no impact on IP Security sessions.

As mobility and multi-homing are functionally equivalent, this section applies equally to either situation.

5. Implementation Considerations

Implementers may use any internal implementation they wish, provided that the external appearance is the same as this implementation approach.

5.1 ILNP Correspondent Cache

When in the Identifier/Locator Split mode, nodes maintain an ILNP Correspondent Cache containing several variables for each correspondent. This cache is described in more detail in [ILNP-Intro]. The ILNP Nonce value is an important part of that cache.

5.2 Mode Indicator

To support the Identifier/Locator Split operating mode, and retain the incremental deployability and backwards compatibility needed, the network layer needs a mode bit in the Transport Control Block (or equivalent for one's implementation) to track which IP sessions are using the classic IPv6 mode, and which IP

sessions are using the Identifier/Locator Split mode.

If a given transport-layer session is in the I/L Split Mode, then an entry corresponding to that session will exist in the ILNP Correspondent Cache. Note that multiple transport-layer sessions between a given pair of nodes normally share a single entry in the Correspondent Cache.

5.3 IP Security

Whether or not the I/L-Split Mode is in use, the IPsec subsystem is required to maintain an IPsec Security Association Database (SAD) and also information about which IPsec Selectors apply to traffic received by or sent from the local node. [RFC 4301] By combining the information in the IPsec SAD, of what IPsec Selectors apply, and the ILNP Correspondent Cache, an implementation has sufficient knowledge to apply IPsec properly to both received and transmitted packets.

6. Backwards Compatibility

If a node has been enhanced to support the Identifier/Locator Split operating mode, that node's fully-qualified domain name SHOULD have one or more ID records and also one or more Locator (i.e. L64 or LP) records associated with it in the DNS.

When a host ("initiator") initiates a new IP session with a correspondent ("responder"), it normally will perform a DNS lookup to determine the address(es) of the responder. A host that has been enhanced to support the Identifier/ Locator Split operating mode normally will look for Identifier ("ID") and Locator ("L64") records in any received DNS replies. DNS servers that support ID and Locator (i.e., L64 or LP) records SHOULD include them (when they exist) as additional data in all DNS replies to queries for DNS AAAA records.

If the initiator supports the I/L Split mode and from DNS data learns that the responder also supports the I/L Split mode, then the initiator MUST generate an unpredictable nonce value, MUST store that value in the local correspondent cache, and MUST include the Nonce Destination Option in its initial packet(s) to the responder. The IETF has provided advice on generating cryptographically random numbers, such as this nonce value. [RFC 4086]

If the responder supports the I/L Split mode and receives initial packet(s) containing the Nonce Destination Option, the responder will thereby learn that the initiator supports the I/L Split mode

and the responder will also operate in I/L Split mode for this new IP session.

If the responder supports the I/L Split mode and receives initial packet(s) NOT containing the Nonce Destination Option, the responder will thereby learn that the initiator does NOT support the I/L Split mode and the responder will operate in classic IPv6 mode for this new IP session.

If the responder does not support the I/L Split mode and receives initial packet(s) containing the Nonce Destination Option, the responder MUST drop the packet and MUST send an ICMP "Parameter Problem" error message back to the initiator.[RFC 4443]

If the initiator EITHER does not receive a response from the responder in a timely manner (e.g. within the applicable TCP timeout for a TCP session) and also does not receive an ICMP Unreachable error message for that packet, OR if the initiator receives an ICMP Parameter Problem error message for that packet, then the initiator infers that the responder is not able to support the I/L Split Operating mode. In this case, the initiator should try again to create the new IP session, but this time use classic IPv6 mode and hence MUST NOT include the Nonce Destination Option.

7. Security Considerations

The Nonce Destination Option is used ONLY for IPv6 sessions using Identifier/Locator split mode, because this option is part of the backwards-compatibility and incremental-deployment approach for the Identifier-Locator Network Protocol (ILNP).

The Nonce Destination Option only seeks to provide protection against off-path attacks on an IP session. Ordinary IPv6 is vulnerable to on-path attacks unless the IP Authentication Header or IP Encapsulating Security Payload are in use. This option exists to provide equivalent protection for non-IPsec traffic when the Identifier/Locator Split mode is in use for an IP session.

When the Identifier/Locator (I/L) split mode is in use for an existing IP session, the Nonce Destination Option MUST be included in any ICMP control messages (e.g. ICMP Unreachable, ICMP Locator Update) sent with regard to that ILNPv6 session, even if IP Security is also in use for that session.

When in the I/L Split operating mode for an existing IPv6 session, any ICMP control messages received without a Nonce

Destination Option MUST be discarded as forgeries. This security event SHOULD be logged in accordance with local security logging policies, including details of the received packet (i.e. Source Locator, Source Identifier, Destination Locator, Destination Identifier, upper-layer protocol (e.g. TCP, UDP, OSPF) if any, transport-layer port numbers if any, and the date and time the packet was received).

When in the I/L Split operating mode for an existing IPv6 session, ICMP control messages received without a correct nonce value inside the Nonce Destination Option MUST be discarded as forgeries. This security event SHOULD be logged as described above.

Of course, longer nonce values provide greater resistance to random guessing of the nonce value. However, ID/Locator Split mode sessions operating in higher risk environments should use the cryptographic authentication provided by IP Authentication Header. Note that the Nonce Option MUST be present -- even if the IP Authentication Header is in use for a given session.

As a performance optimisation, it is suggested that when both the Nonce Option and IP Security are present in a packet, and the Nonce Option has not been encrypted (e.g. ESP is not in use), that the Nonce Option value be checked for validity before beginning IP Security processing. This minimises the ability of an off-path attacker to force the receipient to perform expensive cryptographic computations on received control packets.

For environments with data at differing Sensitivity Levels operating over common infrastructure (e.g. when the IPv6 CALIPSO is deployed), it is recommended that the Nonce Option is encrypted by using ESP Transport-Mode or ESP Tunnel-Mode in order to reduce the covert channel bandwidth potential created by the Nonce Option and to prevent a node at one sensitivity level from attacking a session at a different sensitivity level.[RFC 5570] It is further recommended that multi-level secure systems use different nonce values for sessions with different Sensitivity Levels.[RFC 5570]

In all cases, the Nonce Value MUST be unpredictable and cryptographically random. RFC 4086 provides concrete advice on how to generate a suitable nonce value.[RFC 4086]

As this is an option within the IPv6 Destination Option Header, rather than an option within the IPv6 Hop-by-Hop Option Header, the presence of this option in an IPv6 packet ought not disturb routers along the path an IP packet containing this option

happens to travel. Further, many modern IP routers (both IPv4 and IPv6) have been explicitly configured to ignore all IP options, even including the "Router Alert" option, when forwarding packets not addressed to the router itself. Reports indicate this has been done to preclude use of IP options as a (Distributed) Denial-of-Service (D)DOS attack vector on backbone routers.

8. IANA Considerations

IANA is requested to assign a new Destination Option Type value (replacing XXX, in Section 2 above).

The Nonce Option MUST NOT change in transit and MUST be included in IP Authentication Header calculations.

Further, if an end system receives a packet containing this option, but does not recognise the option, the end system drops the received packet and if and only if the Destination Address was NOT an IPv6 multicast address the receiving end system sends an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognised Option Type.

9. References

9.1. Normative References

[RFC 2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC 2460] S. Deering & R. Hinden, "Internet Protocol Version 6 Specification", RFC 2460, December 1998.

[RFC 4301] S. Kent & K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC 4302] S. Kent, "IP Authentication Header", RFC 4302, December 2005.

[RFC 4443] A. Conta, S. Deering, M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for IPv6 Specification", RFC 4443, March 2006.

9.2. Informative References

[8+8] M. O'Dell, "8+8 - An Alternate Addressing Architecture for IPv6", Internet-Draft, October 1996.

[GSE] M. O'Dell, "GSE - An Alternate Addressing Architecture for IPv6", Internet-Draft, February 1997.

[ILNP-Intro] Atkinson, R, "ILNP Concept of Operations", draft-rja-ilnp-intro-10.txt, February 2011.

[ILNP-DNS] Atkinson, R, "DNS Resource Records for ILNP", draft-rja-ilnp-dns-10.txt, February 2011.

[ILNP-ICMP] Atkinson, R, "ICMP Locator Update message" draft-rja-ilnp-icmp-10.txt, February 2011.

[RFC 4086] D. Eastlake 3rd, J. Schiller, & S. Crocker, "Randomness Requirements for Security", RFC 4086, June 2005.

[RFC 5570] M. StJohns, R. Atkinson, and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", RFC-5570, July 2009.

ACKNOWLEDGEMENTS

Steve Blake, Saleem Bhatti, Noel Chiappa, Steve Hailes, Joel Halpern, Mark Handley, Volker Hilt, Tony Li, and Yakov Rehkter (in alphabetical order) provided review and feedback on earlier versions of this document. Steve Blake provided an especially thorough review of the entire ILNP document set, which led to significant improvements in this document.

Author's Address:

RJ Atkinson
Consultant
McLean, VA
22102 USA

rja.lists@gmail.com

Expires: 27 JAN 2012