Independent Submission
Request for Comments: 8136
Category: Informational
ISSN: 2070-1721
1 April 2017

B. Carpenter
Univ. of Auckland
R. Hinden
Check Point Software

Additional Transition Functionality for IPv6

Abstract

This document proposes an additional mechanism intended to both facilitate transition from IPv4 to IPv6 and improve the latter's security and privacy.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

In a recent statement [IABv6], the Internet Architecture Board deemed that the Internet Engineering Task Force is expected to "stop requiring IPv4 compatibility in new or extended protocols" and that future work will "optimize for and depend on IPv6". In the interest of promoting these goals, this memo makes an important change to IPv4 node requirements [RFC1122] and adds a missing security feature to IPv6 [RFC2460].

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are not to be interpreted as described in [RFC2119].

2. Required Function of All IPv4 Nodes

To ensure that all routers, firewalls, load balancers, and other forms of middleboxes can readily identify IPv4 packets and deal with them appropriately (selective dropping, switching to the slow path through a router, sending them to the longest path first, etc.), all IPv4 nodes MUST set the security flag defined by [RFC3514] to 1. This should be sufficient to ensure that implementers of dual stack applications prefer IPv6 when given the choice, and that the Happy Eyeballs algorithm [RFC6555] will usually favour the IPv6 path.

3. Security Flag for IPv6 Packets

The above requirement will somewhat nullify the practical effect of the IPv4 security flag for benign traffic, but this disadvantage can readily be overcome by adding an equivalent flag for IPv6; in fact, this is highly desirable to maintain feature equivalence between IPv4 and IPv6. Fortunately, this can easily be achieved since IPv6 supplies so many bits. The solution defined here is that the Security Flag bit for an IPv6 packet is simply the parity of the source address of the packet. In other words, if the source address contains an odd number of 1s, the flag is True; otherwise, it's False. All other considerations for the flag are exactly as described in [RFC3514].

For an interface whose IPv6 address is set by Stateless Address Autoconfiguration [RFC4862], it is the host itself that determines the state of its security flag, by choosing an appropriate Interface Identifier value. Fortunately this is now possible and compatible with [RFC7136], [RFC7217], [RFC7421], and [RFC7721].

For an interface whose IPv6 address is set by DHCPv6 [RFC3315] or manually, the network administrator is free to choose an Interface Identifier that provides the desired security flag that is also compatible with [RFC7721].

An exception case is a link with a 127-bit prefix [RFC6164]. Since there is only one bit available as an Interface Identifier, one end or the other will inevitably have its security flag set, and the other won't. In this case, the node at one end will simply interpret the other end's security flag to mean the opposite of what it says, and vice versa.

Since RFC 6164 is designed for links between routers, in the case where different ISPs are at each end of the link, it is normal operational practice for one ISP to consider the other ISP to be evil.

4. Advanced Solution

In the event that the previous solution proves too simple to deploy in practice, a more advanced solution is also defined. It uses a new IPv6 hop-by-hop User Security Flag Option (UFO).

The UFO is a hop-by-hop option that can be included in any IPv6 packet. Multiple UFOs MUST NOT be present in the packet. The UFO has no alignment requirement. Its format is as follows:

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                 |  Option Type  | Option Length |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | UserSecFlag   |
 +-+-+-+-+-+-+-+-+
```

User Security Flag Option Layout

Option Type

8-bit identifier of the type of option. The option identifier for the User Security Flag Option (0x7g) has not been allocated by the IANA.

Option Length

8-bit unsigned integer. The length of the option (excluding the Option Type and Option Length fields). The value MUST be 1.

UserSecFlag

8-bit unsigned integer. Bit 0 has the functionality defined in [RFC3514]. The other bits are reserved and MUST be zero or one.

4.1. Privacy Extension

The mechanism can be extended to add a privacy flag. With the mechanism of Section 3, the privacy flag could be encoded by using quaternary parity (CRC-2) to obtain an extra bit. However, this would waste considerable amounts of address space and SHOULD NOT be done. With the UFO mechanism, bit 1 of UserSecFlag is defined as the privacy flag. If set, it means that the packet contains private information and MUST NOT be inspected en route. All firewalls, monitoring devices, and government agencies MUST respect this rule. This option is expected to be much more computationally efficient than conventional privacy techniques like IPsec and Transport Layer Security (TLS) as no encryption or key management is required to achieve the desired privacy.

5. Security Considerations

The security considerations of [RFC3514] now apply to IPv6. However, with the security flag being set for all IPv4 packets, there is a risk that all IPv4 traffic will now be treated as a very distributed denial-of-service attack.

Given the recent experience with very large scale DDoS attacks from Internet of Things (IoT) devices like IP Cameras, phishing attacks, malware, etc., that occur on the IPv4 Internet, it is a safe assumption that all IPv4 packets are evil.

Since the mechanism described in Section 3 is compatible with [RFC7721], address privacy is not impacted. Also, with that mechanism, exactly half the IPv6 address space will indicate that the security flag is set, so we can assert that the IPv6 Internet is only half evil.

6. IANA Considerations

This document does not require any IANA actions.

7. References

7.1. Normative References

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <http://www.rfc-editor.org/info/rfc1122>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

[RFC6164] Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "Using 127-Bit IPv6 Prefixes on Inter-Router Links", RFC 6164, DOI 10.17487/RFC6164, April 2011, <http://www.rfc-editor.org/info/rfc6164>.

[RFC6555] Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts", RFC 6555, DOI 10.17487/RFC6555, April 2012, <http://www.rfc-editor.org/info/rfc6555>.

[RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <http://www.rfc-editor.org/info/rfc7136>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <http://www.rfc-editor.org/info/rfc7217>.

7.2. Informative References

[IABv6] IAB, "IAB Statement on IPv6", November 2016, <https://www.iab.org/2016/11/07/iab-statement-on-ipv6/>.

[RFC3514] Bellovin, S., "The Security Flag in the IPv4 Header", RFC 3514, DOI 10.17487/RFC3514, April 2003, <http://www.rfc-editor.org/info/rfc3514>.

[RFC7421] Carpenter, B., Ed., Chown, T., Gont, F., Jiang, S., Petrescu, A., and A. Yourtchenko, "Analysis of the 64-bit Boundary in IPv6 Addressing", RFC 7421, DOI 10.17487/RFC7421, January 2015, <http://www.rfc-editor.org/info/rfc7421>.

[RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <http://www.rfc-editor.org/info/rfc7721>.

Authors' Addresses

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com

Robert M. Hinden
Check Point Software
959 Skyway Road
San Carlos CA 94070
United States of America

Email: bob.hinden@gmail.com