Workgroup: Network Working Group
Internet-Draft:
draft-templin-6man-jumbofrag-01
Updates: RFC2675 (if approved)
Published: 18 November 2021
Intended Status: Standards Track
Expires: 22 May 2022
Authors: F. L. Templin, Ed.
Boeing Research & Technology

IPv6 Packet Identification

Abstract

Unlike Internet Protocol, version 4 (IPv4), Internet Protocol, version 6 (IPv6) does not include an Identification field in the basic packet header. Instead, IPv6 includes a 32-bit Identification field in a Fragment Header extension since the architecture assumed that the sole purpose for the Identification is to support the fragmentation and reassembly process. This document asserts that per-packet Identifications may be useful for other purposes, e.g., to allow recipients to detect spurious packets that may have been injected into the network by an attacker. But, rather than defining a new extension header, this document recommends employing the existing Fragment Header for per-packet identification even if the packet itself appears as an "atomic fragment".

Status of This Memo

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 22 May 2022.

Copyright Notice

Table of Contents

1. Introduction

Unlike Internet Protocol, version 4 (IPv4) [RFC0791], Internet Protocol, version 6 (IPv6) [RFC8200] does not include an Identification field in the basic packet header. Instead, IPv6 includes a 32-bit Identification field in a Fragment Header extension since the architecture assumed that the sole purpose for an Identification is to support the fragmentation and reassembly process. This document asserts that per-packet Identifications may be useful for other purposes, e.g., to allow recipients to detect spurious packets that may have been injected into the network by an attacker. But, rather than defining a new extension header, this document recommends employing the existing Fragment Header for per-packet identification even if the packet itself appears as an "atomic fragment".

Atomic fragments are defined as "IPv6 packets that contain a Fragment Header with the Fragment Offset set to 0 and the M flag set to 0" [RFC6946]. When an IPv6 source includes a Fragment Header (i.e., either in an atomic fragment or in multiple fragments), only the source itself and not an intermediate IPv6 node on the path is permitted to alter its contents. This is mandated in the base IPv6 specification which states "unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path".

IPv6 sources that include a Fragment Header include an unpredictable Identification value with each packet [RFC7739]. If the IPv6 source and destination maintain a "window" of acceptable Identification values, this may allow the destination to discern packets originated by the true IPv6 source from spurious packets injected into the network by an attacker.

This document therefore asserts that IPv6 sources are permitted to include a Fragment Header in their packet transmissions (i.e., whether as atomic fragments or in multiple fragments) as long as they include suitable unpredictable Identification values. This includes IPv6 "jumbograms" (i.e., packets larger than 65,535 octets [RFC2675]) which can only be prepared as atomic fragments since they are not eligible for fragmentation. Since the current jumbogram specification forbids sources from including a Fragment Header of any kind, this document updates [RFC2675].

2. IPv6 Packet Identification

When IPv6 sources and destinations have some way of maintaining "windows" of acceptable Identification values, the destination may be able to examine received packet Identifications to determine whether they likely originated from the source. The AERO [I-D.templin-6man-aero] and OMNI [I-D.templin-6man-omni] specifications discuss methods for maintaining windows of unpredictable values that may reduce attack profiles in some environments.

3. RFC2675 Updates

The following updates to [RFC2675] are requested:

*Section 3, third paragraph, change: "The Jumbo Payload option must not be used in a packet that carries a Fragment header" to: "The Jumbo Payload option must not be used in a packet that carries a non-atomic Fragment header [RFC6946]".

*Section 3, in the list of errors, change: "error: Jumbo Payload option present and Fragment header present" to: "error: Jumbo Payload option present and non-atomic Fragment header present".

*Add [RFC6946] to Informative References.

4. Implementation Status

TBD.

5. IANA Considerations

This document has no IANA considerations.

6. Security Considerations

Communications networking security is necessary to preserve confidentiality, integrity and availability.

7. Acknowledgements

This work was inspired by ongoing AERO/OMNI/DTN investigations.

.

8. References

8.1. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC2675] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, DOI 10.17487/RFC2675, August 1999, <https://www.rfc-editor.org/info/rfc2675>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

8.2. Informative References

[I-D.templin-6man-aero] Templin, F. L., "Automatic Extended Route Optimization (AERO)", Work in Progress, Internet-Draft, draft-templin-6man-aero-36, 25 October 2021, <https://www.ietf.org/archive/id/draft-templin-6man-aero-36.txt>.

[I-D.templin-6man-omni] Templin, F. L. and T. Whyman, "Transmission of IP Packets over Overlay Multilink Network (OMNI) Interfaces", Work in Progress, Internet-Draft, draft-templin-6man-omni-49, 25 October 2021, <https://www.ietf.org/archive/id/draft-templin-6man-omni-49.txt>.

[RFC6946] Gont, F., "Processing of IPv6 "Atomic" Fragments", RFC 6946, DOI 10.17487/RFC6946, May 2013, <https://www.rfc-editor.org/info/rfc6946>.

[RFC7739] Gont, F., "Security Implications of Predictable Fragment Identification Values", RFC 7739, DOI 10.17487/RFC7739, February 2016, <https://www.rfc-editor.org/info/rfc7739>.

Author's Address

Fred L. Templin (editor)
Boeing Research & Technology
P.O. Box 3707
Seattle, WA 98124
United States of America

Email: fltemplin@acm.org