Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 27, 2009

M. Eubanks
Iformata Communications
P. Chimento
Johns Hopkins University Applied Physics Laboratory
February 23, 2009

UDP Checksums for Tunneled Packets
draft-eubanks-chimento-6man-00

Status of this Memo

This Internet-Draft is submitted to IETF 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.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 27, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

We address the problem of computing the UDP checksum on tunneling IPv6 packets when using lightweight tunneling protocols.

Requirements Language

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 [RFC2119].

Table of Contents

1. Introduction

The origin of this I-D is the problem raised by the draft titled "Automatic IP Multicast Without Explicit Tunnels", also known as "AMT". This draft uses UDP as the layer protocol in tunneling packets; that is, the outer packet carrying a tunneled (inner) packet. The draft specifies that for packets carrying tunneled multicast data only, the UDP checksum in the UDP header of the outer packet SHOULD be 0 (See draft-ietf-mboned-auto-multicast-09, Section 6.6). However RFC 2460 (IPv6) explicitly states that IPv6 receivers MUST discard UDP packets with a 0 checksum. So, while sending a UDP packet with a 0 checksum is permitted in IPv4 packets, it is explicitly forbidden in IPv6 packets.

The computation of an additional checksum, when the inner packet(s) are already adequately protected, is seen to be an unwarranted burden on nodes implementing lightweight tunneling protocols.

1.1. Some Terminology

For the remainder of this draft, we discuss only IPv6, since this problem does not exist for IPv4. So any reference to 'IP' should be understood as a reference to IPv6.

Although we will try to avoid them when possible, we may use the terms "tunneling" and "tunneled" as adjectives when describing packets. When we refer to 'tunneling packets' we refer to the outer packet header that provides the tunneling function. When we refer to 'tunneled packets' we refer to the inner packet, i.e. the packet being carried in the tunnel.

1.2. Problem Statement

The argument made by the draft authors is that since multicast packets already have a UDP header with a checksum, there is no additional benefit and indeed some cost to nodes to both compute and

check the UDP checksum of the outer (encapsulating) header. However, Consequently, IPv6 should make an exception to the rule that the UDP checksum MUST not be 0, and allow tunneling protocols to set the checksum field of the outer header only to 0 and skip both the sender and receiver computation.

1.3. Alternate Solutions

1. UDP-lite: Some suggestions on the mailing list have been to use UDP-lite (RFC 3828) [RFC3828]. This solution minimizes computation. For example, if a tunneling protocol were to use UDP-lite with a checksum coverage field of 8 to construct the

outer (tunneling) packet, the only variable quantity for a given tunnel is the packet length of the inner (tunneled) packet, since the IPv6 pseudo-header is otherwise fixed. This is a constant value then added to the inner packet length (which should be known when the outer packet is constructed). This is simply an add and store, and a computation of the pseudo-header checksum when the tunnel is created. The possible objections to this approach are twofold: First, it still involves computation which some view as unnecessary. Second, NAT traversal is a problem for UDP-lite and may cause packet loss.

2. No exception for lightweight tunneling: Retain the IPv6 specification as it stands and do not allow a UDP checksum equal to 0 in an outer IPv6 tunneling packet.

3. Exception for lightweight tunneling: Amend IPv6 to allow a 0 value in the UDP checksum field for leightweight tunneling protocols which allows them to bypass any checksum computation in the outer header if the inner packet is protected. Rules for usage in this case must be developed.

4. Another possibilty is to allow an exception for the AMT protocol only. This may seem undesirable, but it would restrict the implementation of a zero checksum UDP header over IPv6 only to the AMT endpoints. Any misdelivered packets (i.e. arriving at a non-AMT endpoint) would simply be discarded.

1.4. Possible Pitfalls of a change

One potential problem with the approach which allows an exception to the IPv6 UDP checksum rule is that in general, tunneling (outer) IPv6 packets could be encapsulating either IPv6 packets or IPv4 packets. If the inner (tunneled) packet is an IPv4 packet with a 0 UDP checksum, then the neither the inner nor the outer packet will provide any checksum protection. This would likewise be the case if the inner packet were an IPv6 packet produced by another (future) protocol which uses an exception to the IPv6 rule.

Others on the mailing list have pointed out other issues with changing the IPv6 specification to allow a checksum of 0 on the outer packet header. In particular, Matt Mathis points out that some tunneling devices ignore the DF bit and fragment silently. This would allow two fragmented UDP packets to be spliced together and be decapsulated and forwarded by a tunnel endpoint.

One notes also that there is no IPv6 header checksum.

There is also the possibility of deep-inspection firewall devices or

other middleboxes actually checking the UDP checksum field of the outer packet and discarding the tunneling packets. This is would be an issue also for legacy systems which have not implemented the change in the IPv6 specification. So in any case, there may be packet loss of lightweight tunneling packets because of mixed new-rule and old-rule nodes.

1.5. Recommended Solution

There seems to be some general opinion that a UDP checksum of 0 could be allowed on the outer encapsulating packet of a lightweight tunneling protocol. This would imply that UDP endpoints handling that protocol must change their behavior and not discard UDP packets received with a 0 checksum on the outer packet.

Magnus Westerlund proposed some restrictions on using a UDP header checksum of 0. These are:

1. There must be some way to verify the integrity of the inner (tunneled) packet.

2. The tunneling protocol and implementation must not use

fragmentation of the inner packets being carried.

We would suggest the following elaborations of the above restrictions, if a change in the IPv6 specification moves forward:

- An inner IPv4 packet with a UDP checksum equal to 0 must not be tunneled.

- Non-IP inner packets must have a CRC or other mechanism for checking packet integrity.

- Other tunneling protcocols that use the UDP checksum equal to 0 MUST NOT be tunneled themselves, even if more deeply encapsulated packets have checksums or other integrity checking mechanisms.

- We would recommend that general protocol stack implementations do NOT implement this change. The exception should remain restricted to devices serving as endpoints of the lightweight tunneling protocol adopting the change.

In addition, we would recommend that a security analysis be done in order to assess whether any new vulnerabilities are introduced by such a change.

2. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

3. Security Considerations

4. Acknowledgements

5. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3828] Larzon, L-A., Degermark, M., Pink, S., Jonsson, L-E., and G. Fairhurst, "The Lightweight User Datagram Protocol (UDP-Lite)", RFC 3828, July 2004.

Authors' Addresses

Marshall Eubanks
Iformata Communications

Phone:
Fax:
Email: tme@multicasttech.com
URI:

P.F. Chimento
Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723
USA

Phone: +1-443-778-1743
Fax:

Email: Philip.Chimento@jhuapl.edu
URI: