Text messaging to middlebox administrators using ICMP
draft-welzl-icmp-text-middleboxes-00

Abstract

   This document describes the use of an ICMP message to send text
   messages to on-path middleboxes from the endpoints. The text message
   is sent towards a destination but meant to be read by administrators
   of middleboxes along the path to the destination. The goal is to
   improve the user's experience with simple middlebox cooperation.

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 [RFC2119].

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 http://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 January 1, 2016.

Table of Contents

1. Introduction

   Middleboxes such as firewalls do often not cooperate with endpoints.
   Sometimes, services that are important to users at endpoints can be
   unavailable because the necessary communication is blocked as a
   result of a simple policy decision such as "block everything that is
   unknown". This can unnecessarily degrade the user experience.

   The common way for a user to deal with this problem is to use offline
   methods to determine the administrator (e.g. via a phone directory)
   and then use other means of communication (e.g. a phone call or an
   email). However, sometimes, the person in charge of the middlebox
   that created the problem is not known to the user. In this case,
   being able to send a text message that at least reaches the
   problematic device is perhaps better than nothing.

   This document defines a new ICMP message called "Plaintext" in order
   to support the transmission and identification of such text messages.
   These messages can, for example, be generated by a ping-like tool, or
   automatically generated by an application when a requested
   communication does not work. The goal is to improve the user
   experience via simple middlebox cooperation. The message is sent to
   a destination IP address -- preferrably the address with which
   communication did not work as intended -- and meant to be read by
   middleboxes along the path. The hope is that, if a middlebox drops
   the packet, it is the middlebox that the message was meant to reach
   anyway.

2. Specification

   The source host creates an ICMP Plaintext message, encapsulates it in
   an IP packet having source address = IP address of the source host,
   destination address = IP address of the destination host and forwards
   it.

   Upon receipt of this message from the source host, on-path
   middleboxes might read the content, forward the packet without
   reading the content, or drop the packet. Middleboxes SHOULD forward
   ICMP packets carrying an ICMP Plaintext message towards the
   destination. At a middlebox, the information carried in the message
   can be recorded in a log file. The administrator of the middleboxes
   might read the log file at a suitable time and adjust policies for
   some services on its basis, or just ignore the information without
   doing anything.

   If a Plaintext message passes all the way to the destination, the
   destination may log or just ignore the message; it is not the

intended recipient.

No reply is expected to be sent in response to a Plaintext message.

The format of the ICMPv6 [RFC4443] Plaintext message is defined 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Data ...
+-+-+-+-+-
```

IPv6 Fields:

   Destination address: IP address of the destination host.

ICMPv6 Fields:

   Type: TBD1

   Code: Set to 0 by the originator and ignored by the receiver.

   Checksum: Used to detect data corruption in the ICMPv6 message and
   parts of the IPv6 header.

   Data: Zero or more octets of arbitrary data in the ASCII format.

XXX Author's note: future versions of this draft will specify the
ICMPv4 message. XXX

3. Use Cases

Usually ICMP is used by nodes to report errors encountered in
processing packets, and to perform other internet-layer functions,
such as diagnostics. In this document, ICMP is extended to allow
text messages from the endpoints to be communicated to on-path
middleboxes.

Rather than providing a long-winded description of possible use
cases, we present some example messages that an ICMP Plaintext
message might contain and assume that they are self-explanatory about
the actual usage scenario:

"This is Michael Welzl, sitting in office 4164 at IFI. I want to run
videoconferencing software XY that I need for a project I'm in, but

it doesn't seem to work. I think you blocked some UDP ports there.
Not good, please fix and get back to me."

"Hello, I like the WiFi that's being provided at this airport! But
did you notice that there is almost no reception near the C gates in
terminal 3?"

"Dear ISP, I'm trying to run native SCTP here but packets won't pass
through your network it seems. I'm paying a fortune, please let my
packets pass!"

"The lady at the reception said it's fine to use VoIp in this hotel,
but my phone software xy can't connect. Else the network seems to
work fine. Please fix; room 302."

4. IANA Considerations

This document defines a new ICMPv6 informational messages:
             Type: TBD1   Plaintext   (see Section 2)

5. Security Considerations

The ICMP plaintext message is meant to be advisory in nature, and
known to be unreliable. There is no authentification of the origin
of the message, meaning that administrators of middleboxes should not
automatically trust its content. For example, a request to open a
port to support a specific application could originate from a
malicious source.

6. Acknowledgement

TBD.

7. Normative References

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

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control
           Message Protocol (ICMPv6) for the Internet Protocol
           Version 6 (IPv6) Specification", RFC 4443, March 2006.

Authors' Addresses

   Michael Welzl
   University of Oslo
   PO Box 1080 Blindern
   Oslo N-0316
   Norway

   Email: michawe@ifi.uio.no

   Jianjie You
   Huawei
   101 Software Avenue, Yuhua District
   Nanjing 210012
   China

   Email: youjianjie@huawei.com