A. Lakhiani
S. Ostermann
Ohio University

Expiration Date: March 2003
September 2002

A Proposal for ICMP "Authentication Required" Messages

draft-lakhiani-adminprohib-authreqd-02.txt

1. Status of this Memo

2. Abstract

The current ICMP "Destination Unreachable - Communication Administratively Prohibited" message conveys one bit of information: the gateway is administratively filtering your packets. This memo proposes the addition of an ICMP "Authentication Required" response to provide the more specific message that packets are being administratively prohibited until successful authentication.

3. Introduction

There are situations where the ICMP Administratively Denied message may not provide sufficient information to an end host. Specifically, access may be denied only until the successful completion of authentication. Currently there is no standard mechanism for conveying this message back to the host. All the firewall can do is silently drop the packet, send a TCP Reset packet [RFC 793], or send an ICMP "Administratively Prohibited" message. We suggest that a new ICMP code "Authentication Required" be made available. This would be useful to inform the host of lack of authentication. How this information gets back to the user on that host is beyond the scope of this document.

4. Suggested Use

Let us consider an example to better understand the use of this ICMP message. Suppose a host attempts to communicate over a wireless network that requires the user to authenticate himself to a Kerberos [RFC1510] server. While the gateway drops packets coming from this host, it would be useful to send "Authentication Required" ICMP messages back to the host. The user on that host could then contact the Kerberos server to authenticate himself.

In general, these ICMP messages SHOULD only be sent by a gateway that is willing to allow communications through it upon successful completion of authentication. Determining the appropriate authentication mechanism is beyond the scope of this document.

5. Message Format

```
    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 = 3    |   Code = 16   |          Checksum             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           Unused                              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                   Original Message Header                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

   3

Code

   16 = Authentication Required

Checksum

   The checksum is the 16-bit one's complement of the one's complement sum of the ICMP message starting with the ICMP Type.

For computing the checksum, the checksum field should be zero. This checksum may be replaced in the future.

Original Message Header

Historically, every ICMP error message has included the Internet header and at least the first 8 data bytes of the datagram that triggered the error. This is no longer adequate, due to the use of IP-in-IP tunneling and other technologies [RFC1812]. Therefore, the ICMP datagram SHOULD contain as much of the original datagram as possible without the length of the ICMP datagram exceeding 576 bytes. The returned IP header (and user data) MUST be identical to that which was received, except that the router is not required to undo any modifications to the IP header that are normally performed in forwarding that were performed before the error was detected (e.g., decrementing the TTL, or updating options).

Description

The gateway sends a "Destination Unreachable - Authentication Required" message to a host in the situation where it receives datagrams from that host before the host has authenticated itself to the authentication server. This message MUST only be sent by a gateway willing to allow communications from that host through it upon successful authentication.

6. Security Considerations

A malicious user could use this mechanism to trick a user or host into revealing authentication information to unknown servers. On the other hand a client system that does not know anything about the appropriate authentication mechanism to be used may not use the network at all. This could be exploited to launch a denial of service attack. Protection against such attacks SHOULD be employed, but is out of the scope of this document.

7. References

[RFC792] "Internet Control Message Protocol". J. Postel. September 1981.

[RFC793] "Transmission Control Protocol". J. Postel. September 1981.

[RFC1812] "Requirements for IP Version 4 Routers". F. Baker. June 1995.

[RFC1510] "The Kerberos Network Authentication Service (V5)". J.

Kohl, C. Neuman. September 1993.

8. Author Information

Avinash Lakhiani
Ohio University
301, Stocker Center
Athens, OH 45701

EMail: avinash.lakhiani@ohiou.edu

Shawn Ostermann
School of Electrical Engineering and Computer Science
Ohio University
322B, Stocker Center
Athens, OH 45701

EMail: ostermann@cs.ohiou.edu