Network Working Group Michael Richardson mcr@sandelman.ottawa.on.ca
INTERNET-DRAFT Sandelman Software Works
<draft-ietf-ipsec-icmp-options-00.txt> v1.0, September 1998
Expires in six months

Options for handling ICMP messages that must be forwarded

Status of This memo

Abstract

This document discusses three options for securely communicating ICMP messages from one IPsec security gateway to another. This document expands upon section 6 of the IPsec architecture draft.

Table of Contents

1. Introduction

1.1. Definition of terminology

Here is a network of two security gateways, a client node and a server node.

```
                E1---{G1}--{R1}--{G2}--{R2}--E2

           E1 and E2 are end nodes using TCP or UDP.
           G1/G1 are security gateways.
           Rx are routers.
```

There are both application endpoints and security association endpoints, they will be distinguished with the following terms:

E1 is the transport layer originator. TLO

E2 is the transport layer target. TLT

E1/G1
is a network layer originator/target pair. NLO/NLT/

G1/G2
is a network layer originator/target pair.

G2/E2
is a network layer originator/target pair.

In addition, it is necessary to distinguish three interfaces of the security gateways at which a forwarding decision may need to be made:

red interface
   is the interface that is exposed to the Internet
black interface

is the interface that is connected only to the internal network

tunnel interface
is the logical interface that results from a packet traversing an encrypted/authenticated tunnel and then decrypted. In general AH/ESP packets arrive on the red interface, are authenticated/decrypted (i.e. decapulated). The inner packet, once decapsulated can logically be thought to have arrived on a third interface for the purposes of forwarding policy.

1.2. The end-to-end and transport cases

In the case where security gateways are not involved (i.e. the end-to-end case), then the two end nodes (E1,E2) and the black interface can simply be considered to be the on-board protocol stack.

2. Introduction to the problem

The Internet Control Message Protocol (ICMP) is a protocol carried by IP networks that is unlike traditional protocols like TCP, UDP. ICMP deals with meta information about the network. As such, ICMP messages are really an integral part of a TCP/UDP flow and should get a similar treatment by security gateways as the TCP/UDP flows themselves.

Consider a per-host ARCHSEC, section 4.4.2 or per-host keyed SA between G1 and G2 on behalf of hosts E1 and E2. For reasons outlined in SMB96, it is should be considered typical for gateways to implement per-host or per-port keying.

Gateway G2 can receive ICMP messages from four places: G1, R1, R2 and E2. Some of these hosts should legitimately be able to send ICMP messages to host E1 or host E2. ICMPIPSECV4 and ICMPIPSECV6 makes a determination of which of these hosts may be able to send which kinds of ICMP messages.

This document describes three possible mechanisms by which gateways G1 and G2 may arrange for these reasonable ICMP message to be related to either hosts E1 or E2.

3. Why is this not a simple problem

The IPsec SPD defined in ARCHSEC and negotiated by IKE Pip98, provides for a set of selectors to determine the policy for determining admission into an IPsec SA. An ICMP message from E2 to E1, from R2 to E1 and from G2 to E1 will not satisfy the admission policy of G2.

Trivially G2 could be modified to permit ICMP messages to be transmitted if they arrive on its black interface, or are generated internally. However, upon exit from the tunnel at G1, G1 would consider these ICMP messages to be violations of the SPD and would refuse to forward them.

It is for this reason that a more sophisticated solution must be described, standardized and possibly negotiated with IKE.

Four methods of handling ICMP messages are described herein:

discard
the ICMP message is dropped

explicit ICMP SA
where a seperate SA is established for ICMP messages.

implicit ICMP SA
where the selector mechanism is modified to accept ICMP messages.

ISAKMP
where the pre-existing ISAKMP SA is used to relay information that would normally be carried by ICMP.

4. Discard

The ICMP packet is dropped. The section on that type may give suggestions about other actions that may be desireable for heuristic reasons (i.e. do an PMTU probe), however, a compliant system may completely ignore this ICMP packet.

5. ICMP SA

Upon receiving an ICMP message from R2 or E2, G2 forward it using t an SA configured to accept ICMP messages of this type/code. If no such SA exists, it should, policy permitting, be created and negotiated with IKE.

The proposal parameters for this SA, if not explicitely configured, should be at least as strong as any other SA that is currently being used between the set of end-points. In particular, if encryption (ESP) is being used for any data might be exchanged by the two security gateways, then the same or better encryption should be used for this SA. This restriction is because some ICMP messages echo parts of an offending packet as part of their error processing. Should a weaker encryption algorithm (or no encryption) be used, then data may get revealed.

The SPD for this SA should be configured to accept the union of all sources and destinations for which communication is currently configured.
The creation and subsequent use of this SA may reveal patterns of traffic which one would not always want to reveal.

6. Implicit ICMP

Upon receiving an ICMP message from R2 or E2, G2 forward it using the SA-pair that was used to send the offending packet. The difficulty is in finding the right SA to associate with the ICMP message.

In many cases it is possible to use the copied packet that ICMP messages will returns as a payload. The data contained as payload of the ICMP

message is to be treated as a packet. The tunnel exit SPD is to be applied to this packet. This will result in the incoming SA on which the packet arrived. The corresponding outgoing SA should then be used to send the packet.

At G1, (the other end of the tunnel), the ICMP message will be received. It will fail the exit criteria of the tunnel. Noting that it is an ICMP message of a type that should be put through the tunnel, G1 should be able to again use the contained packet to lookup at SA. It can then verify that the ICMP packet was received using the corresponding incoming SA.

As an alternative, G2 could take the offending packet from the ICMP message and swap the src/dst and src-port/dst-port and attempt to locate an SA based upon this information.

7. ISAKMP ICMP

Upon receiving an ICMP message from R2 or E2, G2 does not forward it. Instead, it forwards this packet via the key management interface to the key management system. The key management daemon will send an ISAKMP Notify message to the other end. The definition of appropriate Notify messages is left to the individual ICMP messages.

8. Security Considerations:

This entire document discusses a security protocol.

9. References:

RFC-1825
R. Atkinson, "Security Architecture for the Internet Protocol", RFC-1825, August 1995.

ICMPIPSEC
M. Richardson, "Options for handling ICMP messages that must be forwarded" work in progress: draft-ietf-ipsec-icmp-options-00.txt, September 1998

ICMPIPSECV4
M. Richardson, "IPv4 ICMP messages and IPsec security gateways" work in progress: draft-ietf-ipsec-icmp-handle-v4.txt, September 1998

ICMPIPSECV6
M. Richardson, "IPv6 ICMP messages and IPsec security gateways" work in progress: draft-ietf-ipsec-icmp-handle-v6-00.txt, September 1998

ARCHSEC

R. Atkinson, S. Kent, "Security Architecture for the Internet Protocol", work in progress: draft-ietf-ipsec-arch-sec-07.txt, July 1998

RFC-1191
J. Mogul, S. Deering, "Path MTU Discovery", RFC-1191, November 1990.

KSM-AH
New AH draft.

Gupta97-1
V. Gupta, S. Glass, "Firewall Traversal for Mobile IP: Goals and Requirements", draft-ietf-mobileip-ft-req-00.txt, work in progress: Jan. 20, 1997

Gupta97-2
V. Gupta, S. Glass, "Firewall Traversal for Mobile IP: Guidelines for Firewalls and Mobile IP entities", draft-ietf-mobileip-firewall-trav-00.txt, work in progress: March 17, 1997

RFC-1256
S. Deering, "ICMP Router Discovery Messages." Sep-01-1991.

RFC-1885
A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)." December 1995.

RFC-0791
J. Postel, "Internet Protocol." Sep-01-1981.

RFC-0792
J. Postel, "Internet Control Message Protocol.", Sep-01-1981.

RFC-0950
J.C. Mogul, J. Postel, "Internet Standard Subnetting Procedure." Aug-01-1985.

Pip98
Piper, D., "The Internet IP Security Domain Of Interpretation for ISAKMP", version 8, draft-ietf-ipsec-ipsec-doi-08.txt.

IKE
Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)," draft-ietf-ipsec-isakmp-oakley-06.txt.

9.1. Author's Address

Michael C. Richardson
Solidum Systems Corporation
940 Belfast Road
Ottawa, ON K1G 4A2
Canada

Telephone: +1 613 244-4804

EMail: mcr@sandelman.ottawa.on.ca

9.2. Expiration and File Name

This draft expires February 1999

Its file name is draft-ipsec-icmp-options-00.txt