

Network Working Group
Request for Comments: 2521
Category: Experimental

P. Karn
Qualcomm
W. Simpson
DayDreamer
March 1999

ICMP Security Failures Messages

Status of this Memo

This document defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). Copyright (C) Philip Karn and William Allen Simpson (1994-1999). All Rights Reserved.

Abstract

This document specifies ICMP messages for indicating failures when using IP Security Protocols (AH and ESP).

Table of Contents

1.	Introduction	1
2.	Message Formats	1
2.1	Bad SPI	2
2.2	Authentication Failed	2
2.3	Decompression Failed	2
2.4	Decryption Failed	2
2.5	Need Authentication	3
2.6	Need Authorization	3
3.	Error Procedures	3
	SECURITY CONSIDERATIONS	4
	HISTORY	5
	ACKNOWLEDGEMENTS	5
	REFERENCES	5
	CONTACTS	6
	COPYRIGHT	7

1. Introduction

This mechanism is intended for use with the Internet Security Protocols [RFC-1825 et sequitur] for authentication and privacy. For statically configured Security Associations, these messages indicate that the operator needs to manually reconfigure, or is attempting an unauthorized operation. These messages may also be used to trigger automated session-key management.

The datagram format and basic facilities are already defined for ICMP [RFC-792].

Up-to-date values of the ICMP Type field are specified in the most recent "Assigned Numbers" [RFC-1700]. This document concerns the following values:

40 Security Failures

2. Message Formats

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Code   |           Checksum           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Reserved           |           Pointer           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
~   Original Internet Headers + 64 bits of Payload   ~
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type 40

Code Indicates the kind of failure:

- 0 = Bad SPI
- 1 = Authentication Failed
- 2 = Decompression Failed
- 3 = Decryption Failed
- 4 = Need Authentication
- 5 = Need Authorization

Checksum Two octets. The ICMP Checksum.

Reserved Two octets. For future use; MUST be set to zero

when transmitted, and MUST be ignored when received.

Pointer Two octets. An offset into the Original Internet Headers that locates the most significant octet of the offending SPI. Will be zero when no SPI is present.

Original Internet Headers ...

The original Internet Protocol header, any intervening headers up to and including the offending SPI (if any), plus the first 64 bits (8 octets) of the remaining payload data.

This data is used by the host to match the message to the appropriate process. If a payload protocol uses port numbers, they are assumed to be in the first 64-bits of the original datagram's payload.

Usage of this message is elaborated in the following sections.

2.1. Bad SPI

Indicates that a received datagram includes a Security Parameters Index (SPI) that is invalid or has expired.

2.2. Authentication Failed

Indicates that a received datagram failed the authenticity or integrity check for a given SPI.

Note that the SPI may indicate an outer Encapsulating Security Protocol when a separate Authentication Header SPI is hidden inside.

2.3. Decompression Failed

Indicates that a received datagram failed a decompression check for a given SPI.

2.4. Decryption Failed

Indicates that a received datagram failed a decryption check for a given SPI.

2.5. Need Authentication

Indicates that a received datagram will not be accepted without additional authentication.

In this case, either no SPI is present, or an unsuitable SPI is present. For example, an encryption SPI without integrity arrives from a secure operating system with mutually suspicious users.

2.6. Need Authorization

Indicates that a received datagram will not be accepted because it has insufficient authorization.

In this case, an authentication SPI is present that is inappropriate for the target transport or application. The principle party denoted by the SPI does not have proper authorization for the facilities used by the datagram. For example, the party is authorized for Telnet access, but not for FTP access.

3. Error Procedures

As is usual with ICMP messages, upon receipt of one of these error messages that is uninterpretable or otherwise contains an error, no ICMP error message is sent in response. Instead, the message is silently discarded. However, for diagnosis of problems, a node SHOULD provide the capability of logging the error, including the contents of the silently discarded datagram, and SHOULD record the event in a statistics counter.

On receipt, special care MUST be taken that the ICMP message actually includes information that matches a previously sent IP datagram. Otherwise, this might provide an opportunity for a denial of service attack.

The sending implementation MUST be able to limit the rate at which these messages are generated. The rate limit parameters SHOULD be configurable. How the limits are applied (such as, by destination or per interface) is left to the implementor's discretion.

Security Considerations

When a prior Security Association between the parties has not expired, these messages SHOULD be sent with authentication.

However, the node MUST NOT dynamically establish a new Security Association for the sole purpose of authenticating these messages. Automated key management is computationally intensive. This could be used for a very serious denial of service attack. It would be very easy to swamp a target with bogus SPIs from random IP Sources, and have it start up numerous useless key management sessions to authentically inform the putative sender.

In the event of loss of state (such as a system crash), the node will need to send failure messages to all parties that attempt subsequent communication. In this case, the node may have lost the key management technique that was used to establish the Security Association.

Much better to simply let the peers know that there was a failure, and let them request key management as needed (at their staggered timeouts). They'll remember the previous key management technique, and restart gracefully. This distributes the restart burden among systems, and helps allow the recently failed node to manage its computational resources.

In addition, these messages inform the recipient when the ICMP sender is under attack. Unlike other ICMP error messages, the messages provide sufficient data to determine that these messages are in response to previously sent messages.

Therefore, it is imperative that the recipient accept both authenticated and unauthenticated failure messages. The recipient's log SHOULD indicate when the ICMP messages are not validated, and when the ICMP messages are not in response to a valid previous message.

There is some concern that sending these messages may result in the leak of security information. For example, an attacker might use these messages to test or verify potential forged keys. However, this information is already available through the simple expedient of using Echo facilities, or waiting for a TCP 3-way handshake.

The rate limiting mechanism also limits this form of leak, as many messages will not result in an error indication. At the very least, this will lengthen the time factor for verifying such information.

History

The text has been extensively reviewed on the IP Security mailing list, in January and February of 1995 and again in December 1995. The specification is stable, and was forwarded to the IESG by the authors for IETF Last Call as a Proposed Standard in March 1996. There have been several implementations.

Acknowledgements

Some of the text of this specification was derived from "Requirements for Internet Hosts -- Communication Layers" [RFC-1122] and "Requirements for IP Version 4 Routers" [RFC-1812].

Naganand Doraswamy and Hilarie Orman provided useful critiques of earlier versions of this document.

Stimulating comments were also received from Jeffrey Schiller.

Special thanks to the Center for Information Technology Integration (CITI) for providing computing resources.

References

- [RFC-792] Postel, J., "Internet Control Message Protocol", STD 5, September 1981.
- [RFC-1122] Braden, R., Editor, "Requirements for Internet Hosts -- Communication Layers", STD 3, USC/Information Sciences Institute, October 1989.
- [RFC-1700] Reynolds, J., and Postel, J., "Assigned Numbers", STD 2, USC/Information Sciences Institute, October 1994.
- [RFC-1812] Baker, F., Editor, "Requirements for IP Version 4 Routers", Cisco Systems, June 1995.
- [RFC-1825] Atkinson, R., "Security Architecture for the Internet Protocol", Naval Research Laboratory, July 1995.

Contacts

Comments about this document should be discussed on the photuris@adk.gr mailing list.

Questions about this document can also be directed to:

Phil Karn
Qualcomm, Inc.
6455 Lusk Blvd.
San Diego, California 92121-2779

karn@qualcomm.com
karn@unix.ka9q.ampr.org (preferred)

William Allen Simpson
DayDreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

wsimpson@UMich.edu
wsimpson@GreenDragon.com (preferred)

Full Copyright Statement

Copyright (C) The Internet Society (1999). Copyright (C) Philip Karn and William Allen Simpson (1994-1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards (in which case the procedures for copyrights defined in the Internet Standards process must be followed), or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING (BUT NOT LIMITED TO) ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

