Network Working Group
Request for Comments: 2946
Category: Standards Track

T. Ts'o
VA Linux Systems

September 2000

Telnet Data Encryption Option

Status of this Memo

Copyright Notice

Abstract

This document describes a the telnet encryption option as a generic method of providing data confidentiality services for the telnet data stream. While this document summarizes currently utilized encryption types and codes, it does not define a specific encryption algorithm. Separate documents are to be published defining implementations of this option for each encryption algorithm.

1. Command Names and Codes

ENCRYPT 38

Encryption Commands	
IS	0
SUPPORT	1
REPLY	2
START	3
END	4
REQUEST-START	5
REQUEST-END	6
ENC_KEYID	7
DEC_KEYID	8

Encryption Types	
NULL	0
DES_CFB64	1
DES_OFB64	2

DES3_CFB64	3
DES3_OFB64	4
CAST5_40_CFB64	8
CAST5_40_OFB64	9
CAST128_CFB64	10
CAST128_OFB64	11

Following historical practice, future encryption type numbers will be assigned by the IANA under a First Come First Served policy as outlined by RFC 2434 [3]. Despite the fact that authentication type numbers are allocated out of an 8-bit number space (as are most values in the telnet specification) it is not anticipated that the number space is or will become in danger of being exhausted. However, if this should become an issue, when over 50% of the number space becomes allocated, the IANA shall refer allocation requests to either the IESG or a designated expert for approval.

2. Command Meanings

IAC WILL ENCRYPT

The sender of this command is willing to send encrypted data.

IAC WONT ENCRYPT

The sender of this command refuses to send encrypted data.

IAC DO ENCRYPT

The sender of this command is willing to receive encrypted data.

IAC DONT ENCRYPT

The sender of this command refuses to accept encrypted data.

IAC SB ENCRYPT SUPPORT encryption-type-list IAC SE

The sender of this command is stating which types of encryption it will support. Only the side of the connection that is DO ENCRYPT may send the SUPPORT command. The current types of encryption are listed in the current version of the Assigned Numbers document [1].

The encryption-type-list may only include types which can actually be supported during the current session. If ENCRYPT is negotiated in conjunction with AUTH the SUPPORT message MUST NOT be sent until after the session key has been determined. Otherwise,

it is impossible to know if the selected encryption type can be properly initialized based upon the type and length of the key that is available."

IAC SB ENCRYPT IS encryption-type ... IAC SE

The sender of this command is stating which type of encryption to use, and any initial data that is needed. Only the side of the connection that is WILL ENCRYPT may send the IS command to initialize the encryption-type scheme.

IAC SB ENCRYPT REPLY encryption-type ... IAC SE

The sender of this command is continuing the initial data exchange in order to initialize the encryption-type scheme. Only the side of the connection that is DO ENCRYPT may send the REPLY command.

IAC SB ENCRYPT START keyid IAC SE

The sender of this command is stating that all data following the command in the data stream will be be encrypted via the previously negotiated method of data encryption. Only the side of the connection that is WILL ENCRYPT may send the START command.

The keyid is a variable length field. It is used by various encryption mechanisms to identify which encryption key is to be used, when multiple encryption keys might be known on either side of the connection. The keyid field is encoded with the most significant byte first, and a keyid value of zero is reserved to indicate the default encryption key (this would typically be an encryption key derived during authentication, with the AUTHENTICATION option). The keyid field must be at least one byte long. The only valid values for "keyid" will be those that have been received in a DEC_KEYID command.

IAC SB ENCRYPT END IAC SE

The sender of this command is stating that all data following the command in the data stream will not be encrypted. Only the side of the connection that is WILL ENCRYPT may send the END

IAC SB ENCRYPT REQUEST-START keyid IAC SE

The sender of this command requests that the remote side begin encryption of the telnet data stream. Only the side of the connection that is DO ENCRYPT may send the REQUEST-START command. The keyid is only advisory, and my be omitted.

IAC SB ENCRYPT REQUEST-END IAC SE

The sender of this command requests that the remote side stop encryption of the telnet data stream. Only the side of the connection that is DO ENCRYPT may send the REQUEST-END command.

IAC SB ENCRYPT ENC_KEYID keyid IAC SE

The sender of this requests that the remote side verify that "keyid" maps to a valid key; or verifies that the "keyid" received in a DEC_KEYID command is valid. If keyid is omitted, it implies that there are no more known keyids, and that the attempt to find a common keyid has failed. Only the side of the connection that is WILL ENCRYPT may send the ENC_KEYID command.

IAC SB ENCRYPT DEC_KEYID keyid IAC SE

The sender of this requests that the remote side verify that "keyid" maps to a valid key on the remote side; or verifies that the "keyid" received in a ENC_KEYID command is valid. If keyid is omitted, it implies that there are no more known keyids, and that the attempt to find a common keyid has failed. Only the side of the connection that is DO ENCRYPT may send the DEC_KEYID command.

3. Default Specification

The default specification for this option is

WONT ENCRYPT
DONT ENCRYPT

meaning there will not be any encryption of the Telnet data stream.

4. Motivation

The Telnet protocol has no form of protection from some intervening gateway looking at IP packets as they travel through the network. This is especially dangerous when passwords are sent as clear text over the network. This option provides a method for encrypting the data stream.

5. Implementation Rules

Once the Encryption option is in effect, all data in the negotiated direction, including TELNET options, is encrypted. Encryption begins with the octet of data immediately following the "IAC SB ENCRYPT START encryption-type IAC SE" command. Encryption ends after the "IAC SB ENCRYPT END IAC SE" command.

WILL and DO are used only at the beginning of the connection to obtain and grant permission for future negotiations. The ENCRYPT option must be negotiated in both directions.

Once the two hosts have exchanged a WILL and a DO, the sender of the DO ENCRYPT must send a ENCRYPT SUPPORT command to let the remote side know the types of encryption it is willing to accept. In the request, a list of supported encryption schemes is sent. Only the sender of the DO may send a list of supported encryption types (IAC SB ENCRYPT SUPPORT encryption-type-list IAC SE). Only the sender of the WILL may actually transmit encrypted data. This is initiated via the "IAC SB ENCRYPT START IAC SE" command, and terminated via the "IAC SB ENCRYPT END IAC SE" command. If a START is received, and then a second START is received before receiving an END, the second START is ignored.

If the sender of the DO would like the remote side to begin sending encrypted data, it can send the "IAC SB ENCRYPT REQUEST-START IAC SE" command. If the sender of the DO would like the remote side to stop sending encrypted data, it can send the "IAC SB ENCRYPT REQUEST-STOP IAC SE" command.

If the receiver of the SUPPORT command does not support any of the encryption types listed in the SUPPORT command, it should send an "IAC SB ENCRYPT IS NULL IAC SE" to indicate that there are no encryption types in common. It may also send an IAC WONT ENCRYPT command to turn off the ENCRYPT option.

The order of the encryption types in a SUPPORT command must be ordered to indicate a preference for different encryption types, the first type being the most preferred, and the last type the least preferred.

If the ENCRYPT option has been enabled, and encrypted data is being received, the receipt of an "IAC WONT ENCRYPT" implies the receipt of an "IAC SB ENCRYPT END IAC SE", e.g., the Telnet data stream is no longer encrypted.

The following example demonstrates the use of the option:

```
   Host1                              Host2

   [ Host1 requests Host2 negotiate the encryption of data that
     Host2 sends to Host1.  Host2 agrees to negotiate the encryption
     of data that it sends to Host1.  ]
   DO ENCRYPT
                                        WILL ENCRYPT
   [ Host1 requests that Host2 enable encryption as soon as the
     initialization is completed, and informs Host2 that is supports
     DES_CFB64.  ]
   IAC SB ENCRYPT REQUEST-START IAC
   SE
   IAC SB ENCRYPT SUPPORT DES_CFB64
   IAC SE
   [ Host2 sends the initial feed to Host1.  Host1 acknowledges
     receipt of the IV.  ]
                                    IAC SB ENCRYPT IS DES_CFB64
                                    CFB64_IV  144 146 63 229 237 148
                                    81 143 IAC SE
   IAC SB ENCRYPT REPLY DES_CFB64
   CFB64_IV_OK  103 207 181 71 224
   55 229 98 IAC SE
   [ Host2 is now free to start sending encrypted data, and since a
     REQUEST-START was received, it enables encryption.  ]
                                    IAC SB ENCRYPT START IAC SE
   [ All data from Host2 to Host1 is now encrypted.  ]
                                    IAC SB ENCRYPT END IAC SE
   [ All data from Host2 to Host1 is now in clear text again.  ]
```

It is expected that any implementation that supports the Telnet ENCRYPT option will support all of this specification.

6. Security Considerations

The ENCRYPT option used in isolation provides protection against passive attacks, but not against active attacks. In other words, it will provide protection from someone who is just watching the IP packets as they pass through the network. However, an attacker who is able to modify packets in flight could prevent the ENCRYPT option from being negotiated.

This flaw can be remedied by using the Telnet Authentication option alongside the ENCRYPT option. Specifically, setting ENCRYPT_USING_TELOPT in the authentication-type-pair can be used to force that Encryption be negotiated even in the face of active attacks.

In addition, an active attacker can interfere with attempts to start or restart encryption. If encryption is requested by the user, and the client is unable to negotiate enabling or re-enabling encryption, the client must assume that it is being attacked, and MUST immediately terminate the telnet connection.

7. Future directions for Telnet Encryption

The specification defines a method for providing data confidentiality to the telnet data stream. Unfortunately all of the encryption mechanism provided under this option do not provide data integrity, because of the complexity of specifying a protocol which provided integrity services efficiently in a stream-oriented protocol.

The TELNET START_TLS specification provides a scheme which provides confidentiality, integrity, and compression, and future work for telnet encryption should closely examine using this specification. One promising approach would use the anonymous Diffie-Hellman mode of TLS, followed by the telnet AUTHENTICATION option where the authentication mechanism would include the client and server finished messages computed during the TLS negotiation.

8. Acknowledgments

This document was originally written by Dave Borman of Cray Research, with the assistance of Theodore Ts'o of MIT and the IETF Telnet Working Group.

9. References

[1] Reynolds, J. and J. Postel, "Telnet Protocol Specification", STD 8, RFC 854, May 1983.

[2] Ts'o, T. and J. Altman, "Telnet Authentication Option", RFC 2941, September 2000.

[3] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

10. Author's Address

Theodore Ts'o, Editor
VA Linux Systems
43 Pleasant St.
Medford, MA 02155

Phone: (781) 391-3464
EMail: tytso@mit.edu

11. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.