Network Working Group Jeffrey Altman
Internet-Draft Columbia University
draft-altman-telnet-enc-des3-ofb-01.txt February 1999

Telnet Encryption: DES3 64 bit Output Feedback

Status of this Memo

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 RFC 2119.

Abstract

This document specifies how to use the Triple-DES encryption algorithm in output feedback mode with the telnet encryption option.

1. Command Names and Codes

Encryption Type

DES3_OFB64	3

Suboption Commands

OFB64_IV	1
OFB64_IV_OK	2
OFB64_IV_BAD	3

2. Command Meanings

IAC SB ENCRYPT IS DES3_OFB64 OFB64_IV <initial vector> IAC SE

The sender of this command generates a random 8 byte initial vector, and sends it to the other side of the connection using the

OFB64_IV command. The initial vector is sent in clear text. Only the side of the connection that is WILL ENCRYPT may send the OFB64_IV command.

```
IAC SB ENCRYPT REPLY DES3_OFB64 OFB64_IV_OK IAC SE
IAC SB ENCRYPT REPLY DES3_OFB64 OFB64_IV_BAD IAC SE
```

The sender of these commands either accepts or rejects the initial vector received in a OFB64_IV command. Only the side of the connection that is DO ENCRYPT may send the OFB64_IV_OK and OFB64_IV_BAD commands. The OFB64_IV_OK command MUST be sent for backwards compatibility with existing implementations; there really isn't any reason why a sender would need to send the OFB64_IV_BAD command except in the case of a protocol violation where the IV sent was not of the correct length (i.e., 8 bytes).

3. Implementation Rules

Once a OFB64_IV_OK command has been received, the WILL ENCRYPT side of the connection should do keyid negotiation using the ENC_KEYID command. Once the keyid negotiation has successfully identified a common keyid, then START and END commands may be sent by the side of the connection that is WILL ENCRYPT. Data will be encrypted using the DES3 64 bit Cipher Feedback algorithm.

If encryption (decryption) is turned off and back on again, and the same keyid is used when re-starting the encryption (decryption), the intervening clear text must not change the state of the encryption (decryption) machine.

If a START command is sent (received) with a different keyid, the encryption (decryption) machine must be re-initialized immediately following the end of the START command with the new key and the initial vector sent (received) in the last OFB64_IV command.

If a new OFB64_IV command is sent (received), and encryption (decryption) is enabled, the encryption (decryption) machine must be re-ini tialized immediately following the end of the OFB64_IV command with the new initial vector, and the keyid sent (received) in the last START command.

If encryption (decryption) is not enabled when a OFB64_IV command is sent (received), the encryption (decryption) machine must be re-ini tialized after the next START command, with the keyid sent (received) in that START command, and the initial vector sent (received) in this OFB64_IV command.

4. Algorithm

DES3 64 bit Output Feedback

```
                   key1       key2       key3
                    |          |          |
                    v          v          v
                +-------+  +-------+  +-------+
             +->| DES-e |->| DES-d |->| DES-e |-- +
             |  +-------+  +-------+  +-------+   |
             +------------------------------------+
                                                 v
     INPUT ------------------------------------->(+) ----> DATA
```

Given:

iV: Initial vector, 64 bits (8 bytes) long.
Dn: the nth chunk of 64 bits (8 bytes) of data to encrypt (decrypt).
On: the nth chunk of 64 bits (8 bytes) of encrypted (decrypted) output.

V0 = DES-e(DES-d(DES-e(iV, key1),key2),key3)
V(n+1) = DES-e(DES-d(DES-e(Vn, key1),key2),key3)
On = Dn ^ Vn

5. Integration with the AUTHENTICATION telnet option

As noted in the telnet ENCRYPTION option specifications, a keyid value of zero indicates the default encryption key, as might be derived from the telnet AUTHENTICATION option. If the default encryption key negotiated as a result of the telnet AUTHENTICATION option contains less than 16 bytes, then the DES_OFB64 option must not be offered or used as a valid telnet encryption option.

The following rules are to be followed for creating three DES encryption keys based upon the available encrypt key data:

keys_to_use = bytes of key data / DES block size (8 bytes)

where the keys are labeled "key1" through "key6" with "key1" being the first 8 bytes; "key2" the second 8 bytes; ... and "key6" being sixth 8 bytes (if available).

When two keys are available:

- data sent from the server is encrypted with key1, decrypted with key2, and encrypted with key1;

- data sent from the client is encrypted with key2, decrypted with key1, and encrypted with key2

When three keys are available:

- data sent from the server is encrypted with key1, decrypted with key2, and encrypted with key3;

- data sent from the client is encrypted with key2, decrypted with key3, and encrypted with key1

When four keys are available:

- data sent from the server is encrypted with key1, decrypted with key2, and encrypted with key3;

- data sent from the client is encrypted with key2, decrypted with key4, and encrypted with key1

When five keys are available:

- data sent from the server is encrypted with key1, decrypted with key2, and encrypted with key3;

- data sent from the client is encrypted with key2, decrypted with key4, and encrypted with key5

When six keys are available:

- data sent from the server is encrypted with key1, decrypted with key2, and encrypted with key3;

- data sent from the client is encrypted with key4, decrypted with key5, and encrypted with key6

In all cases, the keys used by DES3_OFB64 must have their parity corrected after they are determined using the above algorithm.

Note that the above algorithm assumes that it is safe to use a non-DES key (or part of a non-DES key) as a DES key. This is not necessarily true of all cipher systems, but we specify this behaviour as the default since it is true for most authentication systems in popular use today, and for compatibility with existing implementations. New telnet AUTHENTICATION mechanisms may specify althernative methods for determining the keys to be used for this cipher suite in their specification, if the session key negotiated by that authentication mechanism is not a DES key and and where this algorithm may not be safely used.

6. Security considerations

Encryption using Output Feedback does not ensure data integrity; an active attacker may be able to substitute text, if he can predict the clear-text that was being transmitted.

The tradeoff here is that adding a message authentication code (MAC) will significantly increase the number of bytes needed to send a single character in the telnet protocol, which will impact performance on slow (i.e. dialup) links.

This option was originally drafted back when CPU speeds where not necessarily fast enough to do allow use of CFB. Since then, CPU's have gotten much faster. Given the inherent weaknesses in Output Feedback mode, perhaps it should be deprecated in favor of CFB modes?

7. Acknowledgments

This document was based on the "Telnet Encryption: DES 64 bit Output Feedback" draft originally written by Dave Borman of Cray Research with the assistance of the IETF Telnet Working Group.

Author's Address

Jeffrey Altman, Editor
Columbia University
612 West 115th Street Room 716
New York NY 10025 USA

Phone: +1 (212) 854-1344

EMail: jaltman@columbia.edu

Jeffrey Altman * Sr.Software Designer * Kermit-95 for Win32 and OS/2
The Kermit Project * Columbia University
612 West 115th St #716 * New York, NY * 10025
http://www.kermit-project.org/k95.html * kermit-support@kermit-project.org