

December 15, 2006

Telnet Authentication Option

Status of this memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on 16 July 2007.

Copyright Notice

Copyright (C) The IETF Trust (2006).

Abstract

This document describes the authentication option to the Telnet protocol, [RFC 854](#), as a generic method for negotiating an authentication type and mode including whether encryption should be used and if credentials should be forwarded. While this document summarizes currently utilized commands and types it does not define a specific authentication type. Separate documents are to be published defining each authentication type.

This document updates a previous specification of the Telnet authentication option, [RFC 2941](#), to allow the AUTHENTICATION option to be used in conjunction with the START_TLS option, RFC XXXX.

Conventions used in this document

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](#).

1. Introduction

This document describes the authentication option to the Telnet protocol, [RFC 854](#), as a generic method for negotiating an authentication type and mode including whether encryption should be used and if credentials should be forwarded. While this document summarizes currently utilized commands and types it does not define a specific authentication type. Separate documents are to be published defining each authentication type.

This document updates a previous specification of the telnet authentication option, [RFC 2941](#), to allow the AUTHENTICATION option to be used in conjunction with the START_TLS option, RFC XXXX.

This document consolidates and expands the security considerations section.

2. Command Names and Codes

| | |
|-------------------------|----|
| AUTHENTICATION | 37 |
| Authentication Commands | |
| IS | 0 |
| SEND | 1 |
| REPLY | 2 |
| NAME | 3 |
| Authentication Types | |
| NULL | 0 |
| KERBEROS_V4 | 1 |
| KERBEROS_V5 | 2 |
| SPX* | 3 |
| MINK* | 4 |
| SRP | 5 |
| RSA*[also used by SRA*] | 6 |
| SSL* | 7 |
| [unassigned] | 8 |
| [unassigned] | 9 |
| LOKI* | 10 |
| SSA* | 11 |
| KEA_SJ | 12 |
| KEA_SJ_INTEG | 13 |
| DSS | 14 |
| NTLM* | 15 |

Authentication types followed by (*) were never submitted to the

IETF for consideration as an Internet standard.

| | | |
|------------------------|----|--|
| Modifiers | | |
| AUTH_WHO_MASK | 1 | |
| AUTH_CLIENT_TO_SERVER | 0 | |
| AUTH_SERVER_TO_CLIENT | 1 | |
| | | |
| AUTH_HOW_MASK | 2 | |
| AUTH_HOW_ONE_WAY | 0 | |
| AUTH_HOW_MUTUAL | 2 | |
| | | |
| ENCRYPT_MASK | 20 | |
| ENCRYPT_OFF | 0 | |
| ENCRYPT_USING_TELOPT | 4 | |
| ENCRYPT_AFTER_EXCHANGE | 16 | |
| ENCRYPT_START_TLS | 20 | |
| | | |
| INI_CRED_FWD_MASK | 8 | |
| INI_CRED_FWD_OFF | 0 | |
| INI_CRED_FWD_ON | 8 | |

3. Command Meanings

This document makes reference to a "server" and a "client". For the purposes of this document, the "server" is the side of the connection that performed the passive TCP open (TCP LISTEN state), and the "client" is the side of the connection that performed the active TCP open.

IAC WILL AUTHENTICATION

The client side of the connection sends this command to indicate that it is willing to send and receive authentication information.

IAC DO AUTHENTICATION

The servers side of the connection sends this command to indicate that it is willing to send and receive authentication information.

IAC WONT AUTHENTICATION

The client side of the connection sends this command to indicate that it refuses to send or receive authentication information; the server side must send this command if it receives a DO AUTHENTICATION command.

IAC DONT AUTHENTICATION

The server side of the connection sends this command to indicate that it refuses to send or receive authentication information; the client side must send this command if it receives a WILL AUTHENTICATION command.

IAC SB AUTHENTICATION SEND authentication-type-pair-list IAC SE

The sender of this command (the server) requests that the remote side send authentication information for one of the authentication types listed in "authentication-type-pair-list". The "authentication-type-pair-list" is an ordered list of "authentication-type" pairs. Only the server side (DO AUTHENTICATION) is allowed to send this.

IAC SB AUTHENTICATION IS authentication-type-pair <auth data> IAC SE

The sender of this command (the client) is sending the authentication information for authentication type "authentication-type-pair". Only the client side (WILL AUTHENTICATION) is allowed to send this.

IAC SB AUTHENTICATION REPLY authentication-type-pair <auth data> IAC SE

The sender of this command (the server) is sending a reply to the the authentication information received in a previous IS command. Only the server side (DO AUTHENTICATION) is allowed to send this.

IAC SB AUTHENTICATION NAME remote-user IAC SE

This optional command is sent to specify the account name on the remote host that the user wishes to be authorized to use. Note that authentication may succeed, and the authorization to use a particular account may still fail. Some authentication mechanisms may ignore this command. (See Security Considerations.)

The "authentication-type-pair" is two octets, the first is the authentication type, and the second is a modifier to the type. The authentication type may or may not include built-in encryption. For instance, when the Kerberos 5 authentication type is negotiated encryption must be negotiated with either the Telnet START_TLS or ENCRYPT options [[RFC 2946](#)]. However, the SSL and KEA_SJ authentication types provide an encrypted channel as part of a successful Telnet AUTH option negotiation.

There are currently five one bit fields defined in the modifier. The first two of these bits are processed as a pair, the AUTH_WHO_MASK bit and the AUTH_HOW_MASK bit. There are four possible combinations of these two bits:

AUTH_CLIENT_TO_SERVER
AUTH_HOW_ONE_WAY

The client will send authentication information about the local user to the server. If the negotiation is successful, the server will have authenticated the user on the client side of

the connection.

AUTH_SERVER_TO_CLIENT
AUTH_HOW_ONE_WAY

The server will authenticate itself to the client. If the negotiation is successful, the client will know that it is connected to the server that it wants to be connected to.

AUTH_CLIENT_TO_SERVER
AUTH_HOW_MUTUAL

The client will send authentication information about the local user to the server, and then the server will authenticate itself to the client. If the negotiation is successful, the server will have authenticated the user on the client side of the connection, and the client will know that it is connected to the server that it wants to be connected to.

AUTH_SERVER_TO_CLIENT
AUTH_HOW_MUTUAL

The server will authenticate itself to the client, and then the client will authenticate itself to the server. If the negotiation is successful, the client will know that it is connected to the server that it wants to be connected to, and the server will know that the client is who it claims to be.

The third and fifth bits in the modifier are the ENCRYPT_MASK bits. These bits are used to determine if and how encryption should be enabled. Of the four possible combinations only three are currently defined:

ENCRYPT_OFF

Encryption will not be used for this session. TELOPT ENCRYPT SHOULD NOT be negotiated. This mode MUST be used with all AUTH types that do not provide a shared secret to be used as a session key.

ENCRYPT_USING_TELOPT

Encryption will be negotiated via the use of TELOPT ENCRYPT. Immediately after authentication has completed TELOPT ENCRYPT MUST be negotiated in both directions. This is required to occur before credentials forwarding; other telnet options are negotiated; or any user data is transmitted. A failure to successfully negotiate TELOPT ENCRYPT in either direction MUST result in immediate session termination.

ENCRYPT_AFTER_EXCHANGE

Encryption will be activated in both directions immediately after the successful exchange of the shared secret to be used as the session key. The encryption algorithm to be used MUST be implied by the AUTH type.

ENCRYPT_START_TLS

Encryption is provided by TLS which MUST have been negotiated prior to use of this flag. If TLS has not been previously negotiated, authentication-type-pairs including this flag MUST NOT be offered by the server and MUST NOT be accepted by the client. Authentication methods that support this option MUST verify the TLS Channel Binding data [[RFC 4346](#)] as part of the authentication exchange.

The fourth bit field in the modifier is the INI_CRED_FWD_MASK bit. This bit is either set to INI_CRED_FWD_ON or INI_CRED_FWD_OFF. This bit is set by the client to advise the server to expect forwarded credentials from the client.

INI_CRED_FWD_OFF

The client will not be forwarding credentials to the server. This mode must be used if the selected authentication method does not support credentials forwarding.

INI_CRED_FWD_ON

Once authentication, and perhaps encryption, completes, the client will immediately forward authentication credentials to the server.

The motivation for this advisory bit is that the server may wish to wait until the forwarded credentials have been sent before starting any operating system specific login procedures which may depend on these credentials. Note that credentials forwarding may not be supported by all authentication mechanisms. It is a protocol error to set this bit if the underlying authentication mechanism does not support credentials forwarding.

Credentials forwarding MUST NOT be performed if AUTH_CLIENT_TO_SERVER|AUTH_HOW_ONE_WAY was used since the identity of the server can not be assured. Credentials SHOULD NOT be forwarded if the telnet connection is not protected using some encryption or integrity protection services.

Note that older implementations of the telnet authentication option will not understand the ENCRYPT_MASK and INI_CRED_FWD_MASK bits. Hence any implementation wishing to offer these bits will have to offer authentication type pairs with these bits both set and not set if backwards compatibility is required. (See Security

Considerations.)

4. Default Specification

The default specification for this option is

```
WONT AUTHENTICATION DONT AUTHENTICATION
```

meaning there will not be any exchange of authentication information.

5. Motivation

One of the deficiencies of the Telnet protocol is that in order to log into remote systems, users have to type their passwords, which are passed in clear text through the network. If the connection go through untrusted networks, there is the possibility that passwords will be compromised by someone watching the packets while in transit.

The purpose of the AUTHENTICATION option is to provide a framework for the passing of authentication information through the TELNET session, and a mechanism to enable encryption of the data stream as a side effect of successful authentication or via subsequent use of the telnet ENCRYPT option. This means that: 1) the users password will not be sent in clear text across the network, 2) if the front end telnet process has the appropriate authentication information, it can automatically send the information, and the user will not have to type any password. 3) once authentication has succeeded, the data stream can be encrypted to provide protection against active attacks.

It is intended that the AUTHENTICATION option be general enough that it can be used to pass information for any authentication and encryption system.

6. Implementation Rules

WILL and DO are used only at the beginning of the connection to obtain and grant permission for future negotiations.

The authentication is only negotiated in one direction; the server must send the "DO", and the client must send the "WILL". This restriction is due to the nature of authentication; there are three possible cases; server authenticates client, client authenticates server, and server and client authenticate each other. By only negotiating the option in one direction, and then determining which of the three cases is being used via the suboption, potential ambiguity is removed. If the server receives a "DO", it must respond with a "WONT". If the client receives a "WILL", it must respond with a "DONT".

Once the two hosts have exchanged a DO and a WILL, the server is free to request authentication information. In the request, a list of

supported authentication types is sent. Only the server may send requests ("IAC SB AUTHENTICATION SEND authentication-type-pair-list IAC SE"). Only the client may transmit authentication information via the "IAC SB AUTHENTICATION IS authentication-type ... IAC SE" command. Only the server may send replies ("IAC SB AUTHENTICATION REPLY authentication-type ... IAC SE"). As many IS and REPLY suboptions may be exchanged as are needed for the particular authentication scheme chosen.

If the client does not support any of the authentication types listed in the authentication-type-pair-list, a type of NULL should be used to indicate this in the IS reply. Note that if the client responds with a type of NULL, the server may choose to close the connection.

When the server has concluded that authentication cannot be negotiated with the client it should send IAC DONT AUTH to the client.

The order of the authentication types MUST be ordered to indicate a preference for different authentication types, the first type being the most preferred, and the last type the least preferred.

As long as the server is WILL AUTH it may request authentication information at any time. This is done by sending a new list of supported authentication types. Requesting authentication information may be done as a way of verifying the validity of the client's credentials after an extended period of time or to negotiate a new session key for use during encryption.

7. Integration with TELNET START_TLS option

The Telnet START_TLS option [RFC XXXX] enables the Telnet client and server to negotiate the use of the TLS protocol to secure the connection. TLS is most frequently used with X.509 server-side certificates [[RFC 3280](#)]. When properly verified by the client the TLS session provides strong encryption and protects against a wide range of passive and active attacks. When certificates are not used or not verified by the client, the session (although encrypted) is susceptible to man-in-the-middle attacks. These attacks can be detected by verifying the TLS Channel Binding data [[RFC 4346](#)] during the Telnet AUTHENTICATION protocol exchange. The method for performing this verification is authentication type specific.

8. User Interface

Normally protocol specifications do not address user interface specifications. However, due to the fact that the user will probably want to be able to configure the authentication and encryption and know whether or not the negotiations succeeded, some guidance needs to be given to implementors to provide some minimum level of user control.

The user of the client MUST be able to specify whether or not authentication is to be used, and whether or not encryption is to be used if the authentication succeeds. There SHOULD be at least four settings, REQUIRE, PROMPT, WARN and DISABLE. Setting the authentication switch to REQUIRE means that if the authentication fails, then an appropriate error message must be displayed and the TELNET connection must be terminated. Setting the authentication switch to PROMPT means that if the authentication fails, then an appropriate error message must be displayed and the user must be prompted for confirmation before continuing the TELNET session. Setting the authentication switch to WARN means that if the authentication fails, then an appropriate error message must be displayed before continuing the TELNET session. Setting the authentication switch to DISABLE means that authentication will not be attempted. The encryption switch SHOULD have the same settings as the authentication switch; however its settings are only used when authentication succeeds. The default setting for both switches should be WARN. Both of these switches may be implemented as a single switch, though having them separate gives more control to the user.

The server MUST provide the system administrator the ability to specify whether or not authentication is required and which authentication type pairs should be offered to the client and in what order of preference.

9. Security Considerations

This memo describes a general framework for adding authentication and encryption to the telnet protocol. The actual authentication mechanism is described in the authentication suboption specifications, and the security of the authentication option is dependent on the strengths and weaknesses of the authentication suboption.

The ability to negotiate a common authentication mechanism between client and server is a feature of the authentication option that should be used with caution. When the negotiation is performed, no authentication has yet occurred. Therefore each system has no way of knowing whether or not it is connected to the intended system. An intruder could attempt to negotiate the use of an authentication system which is either weak, or already compromised by the intruder.

It should be noted that the negotiation of the authentication type pair is not protected, thus allowing an attacker to force the result of the authentication to the weakest mutually acceptable method. (For example, even if both sides of the negotiation can accept a "strong" mechanism and a "40-bit" mechanism, an attacker could force selection of the "40-bit" mechanism.) An implementation should therefore only accept an authentication mechanism to be

negotiated if it is willing to trust the resulting channel as being secure.

If the START_TLS option has not been negotiated and the authentication type requires that encryption be enabled as a separate optional negotiation there will be a window of vulnerability from the completion of the AUTH option until the successful negotiation to activate bidirectional encryption. During this window an active attack may be successfully implemented. An active attack is one where the underlying TCP stream can be modified or taken over by the active attacker.

The active attack can be prevented if the server only offers authentication type pairs that include the ENCRYPT_USING_TELOPT or ENCRYPT_START_TLS bits set in the ENCRYPT_MASK field, since both parties will agree that an encryption capability must be successfully negotiated. When the ENCRYPT_USING_TELOPT bit is negotiated, the ENCRYPT option MUST be negotiated immediately following the successful completion of the AUTH option.

Authentication types that link the enabling of encryption as a side effect of successful authentication are not vulnerable to this active attack. The ENCRYPT_AFTER_EXCHANGE bit allows these authentication types to optionally negotiate the activation of encryption.

Another opportunity for active attacks is presented when encryption may be turned on and off without re-authentication. Once encryption is disabled, an attacker may hijack the telnet stream, and interfere with attempts to restart encryption. Therefore, a client SHOULD NOT support the ability to turn off encryption. Once encryption is disabled, if an attempt to re-enable encryption fails, the client MUST terminate the telnet connection.

It is important that in all cases the authentication type pair be integrity protected at the end of the authentication exchange. This must be specified for each authentication type to ensure that the result of the telnet authentication option negotiation is agreed to by both the client and the server. To prevent downgrade attacks authentication type suboptions SHOULD (if possible) include either the entire auth-type pair list; or all of the telnet authentication negotiation exchanges in the integrity checksum.

Each side MUST verify the consistency of the auth-type-pairs in each message received. Any variation in the auth-type-pair MUST be treated as a fatal protocol error.

It should also be noted that the transmission of the username in the IAC SB AUTHENTICATION NAME name IAC SE message is not protected. Implementations should verify the value by a secure method before using this untrusted value when there is a possibility of a man-in-the-middle attack. One method of verifying this value is for the

server to request the USER using the NEW ENVIRONMENT option after mutual authentication has been established [[RFC 1572](#)].

10. Example

The following is an example of use of the option:

| Client | Server |
|--|----------------------------------|
| | IAC DO AUTHENTICATION |
| IAC WILL AUTHENTICATION | |
| [The server is now free to request authentication information.] | |
| | IAC SB AUTHENTICATION SEND |
| | KERBEROS_V5 CLIENT MUTUAL |
| | KERBEROS_V5 CLIENT ONE_WAY IAC |
| | SE |
| [The server has requested mutual Kerberos authentication, but is willing to do just one-way Kerberos authentication. The client will now respond with the name of the user that it wants to log in as, and the Kerberos ticket.] | |
| IAC SB AUTHENTICATION NAME "joe" | |
| IAC SE | |
| IAC SB AUTHENTICATION IS | |
| KERBEROS_V5 CLIENT MUTUAL AUTH 4 | |
| 7 1 67 82 65 89 46 67 7 9 77 0 | |
| 48 24 49 244 109 240 50 208 43 | |
| 35 25 116 104 44 167 21 201 224 | |
| 229 145 20 2 244 213 220 33 134 | |
| 148 4 251 249 233 229 152 77 2 | |
| 109 130 231 33 146 190 248 1 9 | |
| 31 95 94 15 120 224 0 225 76 205 | |
| 70 136 245 190 199 147 155 13 | |
| IAC SE | |
| [The server responds with an ACCEPT command to state that the authentication was successful.] | |
| | IAC SB AUTHENTICATION REPLY |
| | KERBEROS_V5 CLIENT MUTUAL ACCEPT |
| | IAC SE |
| [Next, the client sends across a CHALLENGE to verify that it is really talking to the right server.] | |
| IAC SB AUTHENTICATION IS | |
| KERBEROS_V5 CLIENT MUTUAL | |
| CHALLENGE xx xx xx xx xx xx xx | |
| xx IAC SE | |
| [Lastly, the server sends across a RESPONSE to prove that it really is the right server.] | |
| | IAC SB AUTHENTICATION REPLY |
| | KERBEROS_V5 CLIENT MUTUAL |
| | RESPONSE yy yy yy yy yy yy yy yy |
| | IAC SE |

The following is an example of use of the option with encryption negotiated via telnet ENCRYPT:

| Client | Server |
|--|------------------------------------|
| | IAC DO AUTHENTICATION |
| IAC WILL AUTHENTICATION | |
| [The server is now free to request authentication information.] | |
| | IAC SB AUTHENTICATION SEND |
| | KERBEROS_V5 |
| | CLIENT MUTUAL ENCRYPT_USING_TELOPT |
| | KERBEROS_V5 CLIENT ONE_WAY IAC |
| | SE |
| [The server has requested mutual Kerberos authentication, but is willing to do just one-way Kerberos authentication. In both cases it is willing to encrypt the data stream. The client will now respond with the name of the user that it wants to log in as, and the Kerberos ticket.] | |
| IAC SB AUTHENTICATION NAME "joe" | |
| IAC SE | |
| IAC SB AUTHENTICATION IS | |
| KERBEROS_V5 | |
| CLIENT MUTUAL ENCRYPT_USING_TELOPT | |
| AUTH 4 7 1 67 82 65 89 46 67 7 9 | |
| 77 0 48 24 49 244 109 240 50 208 | |
| 43 35 25 116 104 44 167 21 201 | |
| 224 229 145 20 2 244 213 220 33 | |
| 134 148 4 251 249 233 229 152 77 | |
| 2 109 130 231 33 146 190 248 1 9 | |
| 31 95 94 15 120 224 0 225 76 205 | |
| 70 136 245 190 199 147 155 13 | |
| IAC SE | |
| [The server responds with an ACCEPT command to state that the authentication was successful.] | |
| | IAC SB AUTHENTICATION REPLY |
| | KERBEROS_V5 |
| | CLIENT MUTUAL ENCRYPT_USING_TELOPT |
| | ACCEPT IAC SE |
| [Next, the client sends across a CHALLENGE to verify that it is really talking to the right server.] | |
| IAC SB AUTHENTICATION IS | |
| KERBEROS_V5 | |
| CLIENT MUTUAL ENCRYPT_USING_TELOPT | |
| CHALLENGE xx xx xx xx xx xx xx | |
| xx IAC SE | |
| [The server sends across a RESPONSE to prove that it really is the right server.] | |
| | IAC SB AUTHENTICATION REPLY |
| | KERBEROS_V5 |
| | CLIENT MUTUAL ENCRYPT_USING_TELOPT |
| | RESPONSE yy yy yy yy yy yy yy yy |
| | IAC SE |

[At this point, the client and server begin to negotiate the telnet ENCRYPT option in each direction for a secure channel. If the option fails in either direction for any reason the connection must be immediately terminated.]

The following is an example of use of the option with integrated encryption:

| | |
|---|--------------------------------------|
| Client | Server |
| | IAC DO AUTHENTICATION |
| IAC WILL AUTHENTICATION | |
| [The server is now free to request authentication information.] | IAC SB AUTHENTICATION SEND |
| | KEA_SJ |
| | CLIENT MUTUAL ENCRYPT_AFTER_EXCHANGE |
| | IAC SE |
| [The server has requested mutual KEA authentication with SKIPJACK encryption. The client will now respond with the name of the user that it wants to log in as and the KEA cert.] | |
| IAC SB AUTHENTICATION NAME "joe" | |
| IAC SE IAC SB AUTHENTICATION IS | |
| KEA_SJ | |
| CLIENT MUTUAL ENCRYPT_AFTER_EXCHANGE | |
| '1' CertA Ra IAC SE | |
| [The server responds with its KEA Cert.] | |
| | IAC SB AUTHENTICATION REPLY |
| | KEA_SJ |
| | CLIENT MUTUAL ENCRYPT_AFTER_EXCHANGE |
| | '2' |
| | CertB Rb IVb Encrypt(NonceB) |
| | IAC SE |
| [Next, the client sends across a CHALLENGE to verify that it is really talking to the right server.] | |
| IAC SB AUTHENTICATION IS KEA_SJ | |
| CLIENT MUTUAL ENCRYPT_AFTER_EXCHANGE | |
| '3' IVa Encrypt(NonceB xor | |
| 0x0C18 NonceA) IAC SE | |
| [At this point, the client begins to encrypt the outgoing data stream, and the server, after receiving this command, begins to decrypt the incoming data stream. Lastly, the server sends across a RESPONSE to prove that it really is the right server.] | |
| | IAC SB AUTHENTICATION REPLY |
| | KEA_SJ |
| | CLIENT MUTUAL ENCRYPT_AFTER_EXCHANGE |
| | '4' Encrypt(NonceA xor 0x0C18) |
| | IAC SE |
| [At this point, the server begins to encrypt its outgoing data stream, and the client, after receiving this command, begins to decrypt its incoming data stream.] | |

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

11. Normative References

- [RFC 854] Postel, J. and J. Reynolds, "Telnet Protocol Specification", STD 8, [RFC 854](#), May 1983.
- [RFC 2941] T'so, T. and Altman, J., "Telnet Authentication Option", [RFC 2941](#), September 2000.
- [RFC 2946] Ts'o, T., "Telnet Data Encryption Option", [RFC 2946](#), September 2000.
- [RFC 2434] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998.
- [RFC XXXX] Altman, J., "Telnet START_TLS Option", [draft-altman-telnet-starttls](#)
- [RFC 1572] Alexander, S., "Telnet Environment Option", [RFC 1572](#), January 1994
- [RFC 2119] Bradner, S. "Key words for use in RFCs to Indicate Requirement Levels", [RFC2119](#), March 1997.
- [RFC 4346] Dierks, T. and E. Rescorla. "The Transport Layer Security (TLS) Protocol Version 1.1.", [RFC4346](#), April 2006.
- [RFC 3280] Housley, R., Polk, W., Ford, W., and Solo, D. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC3280](#), April 2002

12. IANA Considerations

The IANA will maintain a registry of Telnet Authentication Option mechanism values.

Following historical practice, future authentication type numbers and authentication modifiers will be assigned by the IANA under a First Come First Served policy as outlined by [RFC 2434](#) [4]. 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. IANA is instructed not to issue new suboption values without submission of documentation of their use.

13. Acknowledgements

[RFC 2941](#) from which this document was derived was edited by Theodore Ts'o and Jeffrey Altman.

Many people have worked on this document over the span of many years. Dave Borman was a document editor and author of much of the original text. Other folks who have contributed ideas and suggestions to this text include: David Carrel, Jeff Schiller, and Richard Basch.

14. Editor

Jeffrey Altman
Secure Endpoints Inc
255 W 94th ST
New York NY 10025 USA

jaltman@secure-endpoints.com

Full Copyright Statement

Copyright (C) The IETF Trust (2006).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an

attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).