Network Working Group
Request for Comments: 1412

K. Alagappan
Digital Equipment Corporation

January 1993

Telnet Authentication: SPX

Status of this Memo

This memo defines an Experimental Protocol for the Internet community. Discussion and suggestions for improvement are requested. Please refer to the current edition of the "IAB Official Protocol Standards" for the standardization state and status of this protocol. Distribution of this memo is unlimited.

1. Command Names and Codes

Authentication Types

SPX	3

Suboption Commands

AUTH	0
REJECT	1
ACCEPT	2

2. Command Meanings

IAC SB AUTHENTICATION IS <authentication-type-pair> AUTH <SPX authentication token> IAC SE

This is used to pass the SPX authentication token to the remote side of the connection. (A document which describes the authentication token syntax is forthcoming.) The first octet of the <authentication-type-pair> value is SPX. The second octet is a modifier to the SPX authentication type.

IAC SB AUTHENTICATION REPLY <authentication-type-pair> ACCEPT <mutual response> IAC SE

This command indicates that the authentication was successful. After an SPX authentication exchange, both sides have securely established a random 8-byte key to be used as the default key for the ENCRYPTION option. If the AUTH_HOW_MUTUAL bit is set in the second octet of the authentication-type-pair, the sender includes the mutual response bytes. The receiver of the ACCEPT command compares the "mutual response" with its expected mutual response.

(A document which describes the mutual response syntax is forth coming.) If the AUTH_HOW_ONE_WAY bit is set in the second octet of the authentication-type-pair, the sender includes zero bytes of mutual response.

IAC SB AUTHENTICATION REPLY <authentication-type-pair> REJECT <optional reason for rejection> IAC SE

This command indicates that the authentication was not successful, and if there is any more data in the sub-option, it is an ASCII text message of the reason for the rejection.

3. Implementation Rules

Every command after the first AUTHENTICATION IS must carry the same set of modifiers (e.g., CLIENT|MUTUAL) for subsequent AUTHENTICATION IS and AUTHENTICATION REPLY commands.

If the second octet of the authentication-type-pair has the AUTH_WHO bit set to AUTH_WHO_CLIENT, then the client sends the initial AUTH command, and the server responds with either ACCEPT or REJECT.

If the second octet of the authentication-type-pair has the AUTH_WHO bit set to AUTH_WHO_SERVER, then the server sends the initial AUTH command, and the client responds with either ACCEPT or REJECT.

4. Examples

User "joe" may wish to log in as user "pete" on machine "foo". If "pete" has set things up on "foo" to allow "joe" access to his account, then the client would send IAC SB AUTHENTICATION NAME "pete" IAC SE IAC SB AUTHENTICATION IS SPX AUTH <joe’s spx authentication token> IAC SE. The server would then authenticate the user as "joe" from the token information, and the server would send back either ACCEPT or REJECT. If mutual authentication is being used, the server would include in the ACCEPT message, a mutual response. The authorization check to see if "pete" is allowing "joe" to use his account is made after the authentication exchange is complete. Therefore, it is possible for the client to receive an ACCEPT response (based on the authentication token), but for joe to be denied access to log in to pete’s account.

```
Client                          Server
                                IAC DO AUTHENTICATION
IAC WILL AUTHENTICATION

[ The server is now free to request authentication information.
  ]

                                IAC SB AUTHENTICATION SEND SPX
                                CLIENT|MUTUAL SPX CLIENT|ONE_WAY
                                IAC SE

[ The server has requested mutual SPX authentication.  If mutual
  authentication is not supported, then the server is willing to
  do one-way SPX authentication.  ]

[ The client will now respond with the name of the user that it
  wants to log in as, and the SPX authentication token.  ]

IAC SB AUTHENTICATION NAME
"pete" IAC SE
IAC SB AUTHENTICATION IS SPX
CLIENT|MUTUAL AUTH <spx
authentication token
information> IAC SE

[ The server responds with an ACCEPT command to state that the
  authentication was successful.  ]

[ If AUTH_HOW_MUTUAL, the server responds with the mutual
  response so the client can verify that it is really talking to
  the right server.  ]

[ If AUTH_HOW_ONE_WAY, the server responds with a NULL mutual
  response, since the client is willing to trust the server
  already.  ]

                                IAC SB AUTHENTICATION REPLY SPX
                                CLIENT|MUTUAL ACCEPT <mutual
                                response> IAC SE
```

Security Considerations

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 talking to the system it intends. An intruder could attempt to negotiate the use of an authentication system which is either weak, or already compromised by the intruder.

Author's Address

Kannan Alagappan
Digital Equipment Corporation
550 King Street, LKG1-2/A19
Littleton, MA 01460

EMail: kannan@sejour.lkg.dec.com

Mailing List: telnet-ietf@CRAY.COM

The working group can be contacted via the current chair:

Steve Alexander
INTERACTIVE Systems Corporation
1901 North Naper Boulevard
Naperville, IL 60563-8895

Phone: (708) 505-9100 x256
EMail: stevea@isc.com