Network Working Group
Internet Draft: Using TLS with IMAP4 and POP3
Document: draft-newman-tls-imappop-01.txt

C. Newman
Innosoft

November 1997

Using TLS with IMAP4 and POP3

Status of this memo

Copyright Notice

Introduction

The TLS protocol [TLS] (formerly known as SSL) provides a way to secure a connection from tampering and evesdropping. Obviously, such security is desirable for IMAP [IMAP4] and POP [POP3]. Although advanced authentication mechanisms [IMAP-AUTH, POP-AUTH] can provide this service with less complexity than TLS, TLS is useful in combination with plaintext password logins and other simple mechanisms as it doesn't require a site to upgrade its authentication database.

The common practice of using a separate port for a secure version of each protocol has a number of disadvantages in the IMAP [IMAP4] and POP [POP3] environment. Rather than using the best security available, it means that clients have to be explicitly configured

to use the separate secure port or suffer the performance loss of probing for active ports. For IMAP, this is even more serious as it would require a new URL scheme which could only be resolved by TLS-enabled clients.

This specification defines extensions to IMAP4 and POP3 which activate TLS. It also defines a set of server security policy response codes for use with IMAP4. The response codes MAY be used independently of the TLS extension.

1. Conventions Used in this Document

The key words "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [KEYWORDS].

Formal syntax is defined using ABNF [ABNF].

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

2. Cipher Suite Requirements

This application profile of TLS follows the standard "Mandatory Cipher Suites" requirement as documented in the TLS specification [TLS]. Implementations MUST NOT assume any other cipher suites are present. It is possible that due to certain government export restrictions some non-compliant versions of this extension could be deployed. Implementations wishing to interoperate with such non-compliant versions MAY offer the TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA mechanism. However, since 40 bit ciphers are known to be vulnerable to attack by current technology, any client which actives a 40 bit cipher MUST NOT indicate to the user that the connection is completely secure from evesdropping.

3. IMAP4 STARTTLS extension

When the TLS extension is present in IMAP4, "STARTTLS" is listed as

a capability in response to the CAPABILITY command. This extension adds a single command, "STARTTLS" to the IMAP4 protocol which is used to begin a TLS negotiation.

3.1. STARTTLS Command

Arguments: none

Responses: no specific responses for this command

Result: OK - begin TLS negotiation
NO - security layer already active
BAD - command unknown or arguments invalid

A TLS negotiation begins immediately after the CRLF at the end of the tagged OK response from the server. The STARTTLS command MAY be used in any state. However, a NO response MAY result if a security layer is already active. Once a client issues a STARTTLS command, it MUST NOT issue further commands until a server response is seen.

If STARTTLS is issued in non-authenticated state, the server remains in non-authenticated state, even if client credentials are supplied during the TLS negotiation. The SASL [SASL] EXTERNAL mechanism MAY be used to authenticate once TLS client credentials are successfully exchanged, but servers supporting the STARTTLS command are not required to support the EXTERNAL mechanism.

The formal syntax for IMAP4 is amended as follows:

```
command_any   =/  "STARTTLS"
```

Example:
```
C: a001 CAPABILITY
S: * CAPABILITY IMAP4rev1 STARTTLS
S: a001 OK CAPABILITY completed
C: a002 STARTTLS
S: a002 OK Begin TLS negotiation now
<TLS negotation begins, futher commands sent under TLS layer>
C: a003 LOGIN joe password
S: a003 OK LOGIN completed
```

4. New IMAP4 response codes

This specification defines three new IMAP4 response codes which MAY be used to communicate server security policy to the client. These MAY be implemented independently of the STARTTLS command.

PASS-EXPIRED
: This occurs on a tagged NO response to an AUTHENTICATE or LOGIN command and indicates the password supplied has expired and needs to be changed.

ENCRYPT-NEEDED
: This occurs on a tagged NO response to an AUTHENTICATE or LOGIN command and indicates that the requested authentication mechanism is only permitted underneath a security layer. The client MAY then issue the STARTTLS command and repeat the same AUTHENTICATE or LOGIN command, or try an AUTHENTICATE command with a stronger mechanism. The client SHOULD record the fact that encryption is needed for that user, server and mechanism combination.

AUTH-TOO-WEAK
: This occurs on a tagged NO response to an AUTHENTICATE or LOGIN command and indicates that the mechanism is too weak and is no longer permitted for that user by site policy. This allows a mechanism to be disabled on a per-user rather than a per-server level which is useful if different users have different security requirements or for transitioning from plaintext LOGIN to a more secure mechanism. The client SHOULD record the fact that the user, server and mechanism combination is no longer permitted.

TRANSITION-NEEDED
: This occurs on a tagged NO response to an AUTHENTICATE command. It indicates that the server has an entry for the specified user in a legacy authentication database but does not yet have credentials to offer the requested mechanism. A client which receives this error code MAY do a one-time login using the LOGIN command or another plaintext mechanism (preferably protected by the STARTTLS command) to initialize

credentials for the requested mechanism.

5. POP3 STARTTLS extension

The POP3 STARTTLS extension adds the STLS command to POP3 servers. If this is implemented, the POP3 extension mechanism [POP3EXT] SHOULD also be implemented to avoid the need for client probing.

STLS

Arguments: none

Restrictions:
MAY be given in any state, but MAY fail if a security layer is already active.

Discussion:
A TLS negotiation begins immediately after the CRLF at the

end of the +OK response from the server. A -ERR response MAY result if a security layer is already active. Once a client issues a STLS command, it MUST NOT issue further commands until a server response is seen.

If STLS is issued in authorization state, the server remains in authorization state, even if client credentials are supplied during the TLS negotiation. The AUTH command [POP3-AUTH] with the EXTERNAL mechanism [SASL] MAY be used to authenticate once TLS client credentials are successfully exchanged, but servers supporting the STLS command are not required to support the EXTERNAL mechanism.

Possible Responses:
+OK -ERR

Examples:
C: STLS
S: +OK Begin TLS negotiation
<TLS negotiation begins>
...
C: STLS

```
            S: -ERR Security Layer already active
```

6. POP3 response codes

This uses the POP3 response codes defined in [POP3EXT].

7. imaps and pop3s ports

Separate "imaps" and "pop3s" ports were registered for use with TLS. Use of these ports is discouraged in favor of the STARTTLS command.

One of the arguments used in favor of the separate port technique is that it simplifies configuration of firewalls which filter by IP port. However, a quality server implementation running on the standard port can be configured to require use of the STARTTLS command or a suitably strong SASL mechanism for non-local connections. This provides superior functionality as the client need not be re-configured for use outside the firewall and simpler, faster non-plaintext SASL mechanisms may be acceptable to many sites for non-local connections.

8. Security Considerations

The mechanisms described in this document only apply to protecting a single connection. Messages are still available to server administrators and usually subject to evesdropping, tampering and forgery when transmitted through SMTP or NNTP. Protecting messages requires an object security mechanism such as PGP MIME [PGP-MIME].

An active attacker for IMAP can remove STARTTLS from the IMAP CAPABILITY list, or cause the POP3 STLS command to fail with a message such as "-ERR Unknown command." In order to detect such an attack, clients SHOULD either warn the user when session protection is not active, or be configurable to refuse to proceed without an acceptable level of security.

If a client uses a weak mechanism which sends the user name at the same time as the authentication credentials, such as IMAP4's LOGIN

command, the ENCRYPT-NEEDED or AUTH-TOO-WEAK error codes will not prevent exposure. For this reason, clients SHOULD record the fact that that user, server and mechanism combination is unacceptable to prevent future exposure or be configurable to try stronger mechanisms or activate encryption first.

An active attacker could cause a bogus TRANSITION-NEEDED response to a stronger authentication mechanism. For this reason, clients SHOULD either activate TLS prior to authentication or get explicit permission from the user prior to using a plaintext mechanism for automated transition.

An attacker might probe for users at a site by trying a strong authentication mechanism which could result in TRANSITION-NEEDED for some users. Strong mechanisms can progress partway through negotiation prior to issuing the TRANSITION-NEEDED failure message in order to avoid this problem.

An attacker might probe for users using the POP3 USER command to probe for AUTH-TOO-WEAK or ENCRYPT-NEEDED. Server implementations could use these error codes for unknown users to defeat this attack. Delaying the error until after the PASS command is supplied would unnecessarily reveal a user's password and thus would be a far more serious problem than probing for users.

An active attacker can always cause a down-negotiation to the weakest authentication mechanism or cipher suite available. For this reason, implementations need to be configurable to refuse weak mechanisms or cipher suites.

9. References

[ABNF] Crocker, "Augmented BNF for Syntax Specifications: ABNF", work in progress.

[IMAIL] Crocker, D., "Standard for the Format of Arpa Internet Text Messages", RFC 822, University of Delaware, August 1982.

<ftp://ds.internic.net/rfc/rfc822.txt>

[IMAP4] Crispin, M., "Internet Message Access Protocol - Version 4rev1", RFC 2060, University of Washington, December 1996.

<ftp://ds.internic.net/rfc/rfc2060.txt>

[IMAP-AUTH] Myers, J., "IMAP4 Authentication Mechanism", RFC 1731, Carnegie-Mellon University, December 1994.

<ftp://ds.internic.net/rfc/rfc1731.txt>

[KEYWORDS] Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, Harvard University, March 1997.

<ftp://ds.internic.net/rfc/rfc2119.txt>

[PGP-MIME] Elkins, M., "MIME Security with Pretty Good Privacy (PGP)", RFC 2015, The Aerospace Corporation, October 1996.

<ftp://ds.internic.net/rfc/rfc2015.txt>

[POP3] Myers, J., Rose, M., "Post Office Protocol - Version 3", RFC 1939, Carnegie Mellon, Dover Beach Consulting, Inc., May 1996.

<ftp://ds.internic.net/rfc/rfc1939.txt>

[POP3EXT] Newman, "POP3 Extension Mechanism and Error Codes", Work in progress.

[POP-AUTH] Myers, "POP3 AUTHentication command", RFC 1734, Carnegie Mellon, December 1994.

<ftp://ds.internic.net/rfc/rfc1734.txt>

[SASL] Myers, "Simple Authentication and Security Layer (SASL)", RFC 2222, Netscape Communications, October 1997.

<ftp://ds.internic.net/rfc/rfc2222.txt>

[TLS] Dierks, Allen, "The TLS Protocol Version 1.0", Work in progress.

10. Full Copyright Statement

11. Author's Address

Chris Newman
Innosoft International, Inc.
1050 Lakes Drive
West Covina, CA 91790 USA

Email: chris.newman@innosoft.com