POP3 over TLS
draft-melnikov-pop3-over-tls-02

Abstract

This document specifies how the Post Office Protocol, Version 3 (POP3) may be secured with Transport Layer Security (TLS) protocol, by establishing TLS connection directly before POP3 transaction. It updates RFC 2595.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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/1id-abstracts.html

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

Copyright and License Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to
1. Introduction

The Post Office Protocol version 3 (POP3), which is defined in RFC 1939 [RFC1939], is an application-layer protocol used by local e-mail clients to retrieve e-mail from a remote server over a simple TCP/IP connection. It supports simple download-and-delete requirements for access to remote mailboxes (also called a maildrop).

As POP3 is employed to transfer sensitive information, there is a need for privacy protection. Transport Layer Security (TLS) [RFC5246] (and its predecessor Secure Sockets Layer (SSL) [RFC6101]) are commonly used for this purpose.

Two ways of protecting POP3 with TLS have been deployed (like 2 ways of securing HTTP [RFC2616]; see below). The first includes establishing TLS layer connection during the POP3 transaction (also known as upgrading to TLS) [RFC2595]. The other one involves establishing TLS connection directly before establishing POP3 transaction. Unlike the former, this way (called "POP3S" throughout this document) has not been previously specified in an RFC. (In the case with HTTP the first way is specified in RFC 2817 [RFC2817]; the second one - in RFC 2818 [RFC2818].)

This document specifies POP3S. It updates RFC 2595 [RFC2595] (see Section 2.5 for justification). This memo also updates the
registration of the TCP well-known port 995, used with POP3S.

RFC 6186 [RFC6186] specifies the way to use DNS SRV records [RFC2782] for locating information about email access services. It supports both POP3S and the aforementioned POP3 upgraded to TLS. For more information, refer to Section 3.3 of RFC 6186.

1.1. Terminology

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 [RFC2119]. Terminology from RFC 1939 [RFC1939] is used in this document.

The "POP3S transaction" refers to the POP3 transaction established as described in Section 2.1.

2. POP3 over TLS Protocol

This section contains the technical definition of POP3 over TLS protocol (POP3S).

2.1. Connection Establishment and User Authentication

This section describes how to establish POP3S transaction.

First, the client first establishes the TCP connection [RFC0793] to the server on the 995 port, or other, if explicitly mentioned. As soon as successful connection is established, the TLS negotiation [RFC5246] SHALL be preformed. RFC nnnn [I-D.melnikov-email-tls-certs] describes the procedure which MUST be followed by the clients to verify the server’s certificate. Upon successful negotiation all data SHALL be sent under TLS layer, as defined in Section 2.2. Unsuccessful TLS negotiation SHALL lead to termination of TCP connection.

As soon as successful TLS layer connection is established, the server sends the greeting line, as defined by RFC 1939. Both the server and the client MUST enter AUTHORIZATION state then.

Next, the client should authorize itself to the server. If there is a bilateral convention between the parties regarding authorization using X.509 certificate, the client SHOULD first try to authorize itself using SASL EXTERNAL mechanism, which is defined in Appendix A of RFC 4422 [RFC4422]. For this purpose, the AUTH command [RFC5034] SHALL be used. (Correspondingly, those servers and clients which support authentication using X.509 certificates MUST support the SASL EXTERNAL mechanism.) Servers that lack configuration to accept an
X.509 client certificate for authentication purposes SHOULD NOT send a CertificateRequest handshake to the client during TLS negotiation.

However, if SASL EXTERNAL authentication fails, or there was no certificate exchange during TLS negotiation, the client MAY either close the connection or try a different authentication mechanism (e.g., USER and PASS commands).

After the client has received the +OK response to the authentication command, both the client and server MUST enter TRANSACTION state, per RFC 1939.

SSL 2.0 MUST NOT be used for POP3S; see RFC 6176 [RFC6176] for details.

2.2. Data Exchange

All the data (explicitly, POP3 commands and responses), upon successful TLS negotiation, SHALL be sent as TLS "application data".

2.3. Connection Closure

TLS provides the possibility for secure connection closure. Therefore, upon POP3S transaction closure, the client SHALL initiate the exchange of TLS close alerts, which should happen before TCP connection termination. When the server receives the TLS close alert, it may be sure that no other data will be sent in this connection. The POP3 client MAY, after sending TLS close alert, terminate its part of connection without waiting for a response from the server.

2.4. Default Port

POP3S uses the default port 995. Section 4 updates the IANA registration for this port.

2.5. Disadvantages of POP3S

Section 7 of RFC 2595 [RFC2595] expresses concerns about use of a separate port for POP3S. The concern about port usage does not apply as port 995 was previously registered. RFC 6186 mitigates the other concerns. The usefulness of POP3S outweighs these flaws so the statement in section 7 of RFC 2595 discouraging use of POP3S is rescinded.

3. Security Considerations

POP3S uses TLS [RFC5246] to provide protection from eavesdropping and

4. IANA Considerations

IANA is asked to update the registration of the TCP well-known port 995 using the following template (see RFC 6335 [RFC6335]):

Service Name: pop3s
Transport Protocol: TCP
Assignee: IETF <iesg@ietf.org>
Contact: IESG <iesg@ietf.org>
Description: POP3 over TLS protocol
Reference: RFC xxxx (this document - note to RFC Editor)
Port Number: 995

5. References

5.1. Normative References

[I-D.melnikov-email-tls-certs]


5.2. Informative References


Appendix A. Acknowledgments

We would like to thank Randall Gellens and Paul Smith for their discussion of, ideas for and suggestions to this document.
Authors’ Addresses

Alexey Melnikov
Isode Limited
5 Castle Business Village
36 Station Road
Hampton, Middlesex  TW12 2BX
UK
EMail: Alexey.Melnikov@isode.com

Chris Newman
Oracle
800 Royal Oaks
Monrovia, CA  91016-6347
US
EMail: chris.newman@oracle.com

Mykyta Yevstifeyev (editor)
8 Kuzovkov St., Apt. 25
Kotovsk
Ukraine
EMail: evnikita2@gmail.com