Abstract

This document specifies how the Post Office Protocol, Version 3 (POP3) may be secured with Transport Layer Security (TLS) protocol, by establishing TLS layer connection directly before POP3 transaction. It updates RFC 1939 and 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 this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
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).

Initially, POP3 was intended to be used "in the clear". But since it is often employed to transfer sensitive information, there is a need to secure POP3 transaction; actually, the only protocol used for this purpose is Transport Layer Security (TLS) [RFC5246] (and its deprecated predecessor Secure Sockets Layer (SSL) [RFC6101]).

Historically, two ways of securing the POP3 connection 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). It is discussed in details in RFC 2595 [RFC2595]. The other one involves establishing TLS connection directly before establishing POP3 transaction. Unlike the first one, this way (called "POP3S" throughout this document) has never been given an official specification. (In the case with HTTP the first way is specified in RFC 2817 [RFC2817]; the second one – in RFC 2818 [RFC2818].)

This memo is to remove this uncertainty; it specifies the POP3S protocol in details. This document updates RFC 1939 [RFC1939]. RFC
RFC 2595 [RFC2595] is also updated by it (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. Among other, it defined the way of mentioning that a particular server supports POP3S. 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 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 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 certificate MUST support SASL EXTERNAL mechanism.)

However, if SASL EXTERNAL authentication fails, or there is no convention on using X.509 certificate for authentication, the client SHALL use some other way to identify itself, e.g. USER and PASS commands.

Anyway, as soon as the client authenticates itself, and the server verifies its credentials, they both enter TRANSACTION state and begin exchanging POP commands and replies.

Please note that per RFC 6176 [RFC6176], neither clients nor servers must perform attempts to negotiate use of SSL 2.0.

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 a response from the server.

2.4. Default Port

Historically, the separate TCP port has been used for POP3S - 995. Therefore if there is no explicit specification of port, the client SHALL connect the server on it. Section 4 of this document updates IANA registration of this port number with reference to this document in the corresponding registry.

2.5. Disadvantages of POP3S

Section 7 of RFC 2595 [RFC2595] contains a few words about the POP3S protocol. It discourages its usage in favor of STLS command, described in it, mainly claiming that POP3S, if implemented, would cause many misunderstandings regarding the need of new URI scheme, separate port numbers, etc. These issues are fully considered; however the usefulness of POP3S certainly overweighs these flaws. This specification updates RFC 2595; however, upon approval of this
document, it does not ban the usage of STLS command described there -
it and POP3S may be continued to be used simultaneously.

3. Security Considerations

The POP3S protocol is primarily aimed to secure POP3 connection.
This is achieved by sending data under TLS layer [RFC5246], that
provides protection from eavesdropping, tampering, or message
forgery. Moreover, one of the POP3S scenarios assumes that TLS
negotiation also serves to authenticate the user agent, which
increases the security level of such authentication.

Other authentication schemes, such as Kerberos [RFC4752] (see Section
2 of this document), are also allowed. Please refer to Security
consideration sections of such authentication schemes’ specifications
for discussion of security issues for such certain authentication
schemes.

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]
Melnikov, A., "Updated TLS Server Identity Check
Procedure for Email Related Protocols", Work in Progress
(draft-melnikov-email-tls-certs), June 2011.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7,
RFC 793, September 1981.
5.2. Informative References


Appendix A. Acknowledgments

We would like to thank Randall Gellens, Chris Newman, 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

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