Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 14, 2017

M. Kuehlewind
ETH Zurich

March 13, 2017

Separating Crypto Negotiation and Communication
draft-kuehlewind-crypto-sep-00

Abstract

Based on the increasing deployment of session resumption mechanisms where cryptographic context can be resumed to transmit application data with the first packet without delay for connection setup and negotiation, this draft proposes a split to separate connections used to set up encryption context and negotiate capabilities from connections used to transmit application data. While cryptographic context and endpoint capabilities need to be be known before encrypted application data can be sent, there is otherwise no technical constraint that the crypto handshake has to be performed on the same transport connection. This document discusses requirements on the cryptographic protocol to establish medium- to long-lived association that can be used by different transport protocols that implement different transport services.

Table of Contents

1. Introduction

New cryptographic and transport protocols increasingly rely on session resumption mechanisms where cryptographic context can be resumed to transmit application data with the first packet without delay for connection setup and negotiation. This draft proposed a split to separate connections that are used to set up encryption context and negotiate capabilities from the connection that is used to transmit application data. In this draft we assume the use of TCP with a TLS-like protocol for cryptographic handshake and negotiation of endpoint capabilities, where TCP provides a fully reliable stream-based transport and the message framing is realized by TLS. However, instead of using the same transport TCP connection for TLS or any new TLS-like protocol, the connection will be closed after the cryptographic handshake and a new transport connection that might not use TCP is open at anytime to transmit the actual application data.

In the case where there is no cryptographic context available when an application expressed the wish to transmit data to a certain endpoint, the connection for crypto negotiation must be established first, immediately before the actual payload connection will be used. In this case, as today for approaches that integrate both the cryptographic handshake and the payload transmission, the application data transmission is delayed until the needed cryptographic context is available. Just using a separate transport connection for these

two actions does not generally introduce any extra delay. However, given that these steps don't have to be performed at the same time, crypto negotiation could even be performed (long) before the application expresses a desire to send data. E.g. an integrated or independent software system could maintain knowledge about endpoints that are likely to be communication points and set up or refresh state any time triggered by external events such as the start up of this system or periodically.

This document discusses high-level requirements for a future TLS-like crypto protocol that provides support for this connection separation as well as possible interfaces between the cryptographic protocol and the transport protocol that is used for the transmission of the application data.

[I-D.moskowitz-sse] proposes a similar approach. However while [I-D.moskowitz-sse] proposes a new protocol to negotiate and maintain long-term cryptographic sessions, this document relies on the use of existing protocols and only discusses requirements for the evolution of these protocols and exchange of information within one endpoint locally.

2. Requirements

2.1. Support for different transport services

[editor's note: this section will discuss requirement for crypto protocols to provide cryptographic context that can support different transport feature e.g. partial or non-reliable transports]

2.2. Cryptographic context lifetime management

[editor's note: this section will discuss lifetime management of long-lived cryptographic associations, e.g. when to set up or refresh state for which endpoint and which transport protocols]

3. Crypto-Transport Interface

There are two basic approaches: either the transport protocol can provide data to the crypto engine and get back an encrypted version of the data to be sent, or the crypto protocol can provide keying material and inform the transport about the negotiated capabilities of the far end and the transport is responsible to perform the encryption set.

4. IANA Considerations

This docuement has on request to IANA.

5. Security Considerations

[editor's note: this section will be added later. However, this document discusses the use of cryptograohic context for transport connections and as such it has security relevant consideration within the whole document.]

6. Acknowledgments

This work is partially supported by the European Commission under Horizon 2020 grant agreement no. 688421 Measurement and Architecture for a Middleboxed Internet (MAMI), and by the Swiss State Secretariat for Education, Research, and Innovation under contract no. 15.0268. This support does not imply endorsement.

7. Informative References

[I-D.moskowitz-sse]
Moskowitz, R., Faynberg, I., Lu, H., Hares, S., and P. Giacomin, "Session Security Envelope", draft-moskowitz-sse-04 (work in progress), October 2016.

Author's Address

Mirja Kuehlewind
ETH Zurich
Gloriastrasse 35
8092 Zurich
Switzerland

Email: mirja.kuehlewind@tik.ee.ethz.ch