A Survey of Transport Security Protocols

draft-pauly-taps-transport-security

Tommy Pauly (tpauly@apple.com)
Colin Perkins (csp@csperkins.org)
Kyle Rose (krose@krose.org)
Christopher A. Wood (cawood@apple.com)

TAPS
Overview

Goals:

• Survey existing transport security protocols
• Extract mandatory and optional features
• Identify (common) interfaces
Scope

What’s in?

- Any transport security protocols - not limited to IETF
- Analysis of existing protocols (in collaboration with Security area)

What’s out?

- Recommendations for specific algorithms
- Constructions of new protocols
History

- IETF 98: Action taken to survey security properties of existing transport security protocols
- IETF 99: draft-pauly-taps-transport-security-survey-00, including: TLS (QUIC + TLS), MinimalT, CurveCP, tcpcrypt, IKEv2+ESP
- IETF 100: Added SRTP (with DTLS) and WireGuard
- IETF 101: Added gQUIC
Methodology

Decouple handshake- and record-specific parts of protocol

• Some protocols (ESP) do not have a handshake

• Some protocols (Noise — omitted) do not have a record or framing layer

Focus on interface of each part, not implementation

• Analogous to transport services [RFC 8095]
Protocols

Application

- (D)TLS, QUIC, MinimalT, CurveCP, SRTP(+DTLS)

Session

- tcpcrypt

Transport

- IKEv2+ESP, WireGuard

Internet
## Handshake Features

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private key interface or injection</td>
<td>Mutual authentication</td>
</tr>
<tr>
<td>Remote authentication</td>
<td>Application-layer feature negotiation</td>
</tr>
<tr>
<td>Source validation</td>
<td>Configuration extensions</td>
</tr>
<tr>
<td></td>
<td>Session caching and management</td>
</tr>
</tbody>
</table>
## Record Features

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-shared key support</td>
<td>Connection mobility</td>
</tr>
<tr>
<td>Segment encryption and</td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Interfaces

- Identity and private keys
- Supported algorithms
- Session cache configuration and management
- Authentication delegation
Handshake Interfaces

- Send handshake messages
- Receive handshake messages
- Identity validation
- Source address validation
- Key update
- Pre-shared key export
Record Interfaces

- Pre-shared key import
- Encrypt application data
- Decrypt application data
- Key expiration
- Transport mobility
Open Issues

Address outstanding Github issues

- Unify document structure [https://github.com/mami-project/draft-pauly-transport-security/issues/16]

- Expand Security Considerations [https://github.com/mami-project/draft-pauly-transport-security/issues/21]

Identify delta between protocol implementations and identified interfaces

- Not all bits of an RFC are implemented, and not all implementation interfaces are standardized
Next Steps

1. Call for WG adoption

2. Continue adding protocols [Issues #3, #4, #5, #6, #7, …]

3. Commence reviews with Security area