Stream: Internet Engineering Task Force (IETF)
RFC: 8922
Category: Informational
Published: October 2020
ISSN: 2070-1721
Authors:
T. Enghardt, *TU Berlin*
T. Pauly, *Apple Inc.*
C. Perkins, *University of Glasgow*
K. Rose, *Akamai Technologies, Inc.*
C. Wood, *Cloudflare*

RFC 8922
A Survey of the Interaction between Security Protocols and Transport Services

Abstract

This document provides a survey of commonly used or notable network security protocols, with a focus on how they interact and integrate with applications and transport protocols. Its goal is to supplement efforts to define and catalog Transport Services by describing the interfaces required to add security protocols. This survey is not limited to protocols developed within the scope or context of the IETF, and those included represent a superset of features a Transport Services system may need to support.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8922.

Copyright Notice

Table of Contents

1. Introduction

Services and features provided by transport protocols have been cataloged in [RFC8095]. This document supplements that work by surveying commonly used and notable network security protocols, and identifying the interfaces between these protocols and both transport protocols and applications. It examines Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), IETF QUIC, Google QUIC (gQUIC), tcpcrypt, Internet Protocol Security (IPsec), Secure Real-time Transport Protocol (SRTP) with DTLS, WireGuard, CurveCP, and MinimaLT. For each protocol, this document provides a brief description. Then, it describes the interfaces between these protocols and transports in Section 4 and the interfaces between these protocols and applications in Section 5.

A Transport Services system exposes an interface for applications to access various (secure) transport protocol features. The security protocols included in this survey represent a superset of functionality and features a Transport Services system may need to support both internally and externally (via an API) for applications [TAPS-ARCH]. Ubiquitous IETF protocols such as (D)TLS, as well as non-standard protocols such as gQUIC, are included despite overlapping features. As such, this survey is not limited to protocols developed within the scope or context of the IETF. Outside of this candidate set, protocols that do not offer new features are omitted. For example, newer protocols such as WireGuard make unique design choices that have implications for and limitations on application usage. In contrast, protocols such as secure shell (SSH) [RFC4253], GRE [RFC2890], the Layer 2 Tunneling Protocol (L2TP) [RFC5641], and Application Layer Transport Security (ALTS) [ALTS] are omitted since they do not provide interfaces deemed unique.

Authentication-only protocols such as the TCP Authentication Option (TCP-AO) [RFC5925] and the IPsec Authentication Header (AH) [RFC4302] are excluded from this survey. TCP-AO adds authentication to long-lived TCP connections, e.g., replay protection with per-packet Message Authentication Codes. (TCP-AO obsoletes TCP MD5 "signature" options specified in [RFC2385].) One primary use case of TCP-AO is for protecting BGP connections. Similarly, AH adds per-datagram authentication and integrity, along with replay protection. Despite these improvements, neither protocol sees general use and both lack critical properties important for emergent transport security protocols, such as confidentiality and privacy protections. Such protocols are thus omitted from this survey.

This document only surveys point-to-point protocols; multicast protocols are out of scope.

1.1. Goals

This survey is intended to help identify the most common interface surfaces between security protocols and transport protocols, and between security protocols and applications.

One of the goals of the Transport Services effort is to define a common interface for using transport protocols that allows software using transport protocols to easily adopt new protocols that provide similar feature sets. The survey of the dependencies security protocols have upon transport protocols can guide implementations in determining which transport protocols are appropriate to be able to use beneath a given security protocol. For example, a security protocol that expects to run over a reliable stream of bytes, like TLS, restricts the set of transport protocols that can be used to those that offer a reliable stream of bytes.

Defining the common interfaces that security protocols provide to applications also allows interfaces to be designed in a way that common functionality can use the same APIs. For example, many security protocols that provide authentication let the application be involved in peer identity validation. Any interface to use a secure transport protocol stack thus needs to allow applications to perform this action during connection establishment.

1.2. Non-goals

While this survey provides similar analysis to that which was performed for transport protocols in [RFC8095], it is important to distinguish that the use of security protocols requires more consideration.

It is not a goal to allow software implementations to automatically switch between different security protocols, even where their interfaces to transport and applications are equivalent. Even between versions, security protocols have subtly different guarantees and vulnerabilities. Thus, any implementation needs to only use the set of protocols and algorithms that are requested by applications or by a system policy.

Different security protocols also can use incompatible notions of peer identity and authentication, and cryptographic options. It is not a goal to identify a common set of representations for these concepts.

The protocols surveyed in this document represent a superset of functionality and features a Transport Services system may need to support. It does not list all transport protocols that a Transport Services system may need to implement, nor does it mandate that a Transport Service system implement any particular protocol.

A Transport Services system may implement any secure transport protocol that provides the described features. In doing so, it may need to expose an interface to the application to configure these features.

2. Terminology

The following terms are used throughout this document to describe the roles and interactions of transport security protocols (some of which are also defined in [RFC8095]):

Transport Feature: a specific end-to-end feature that the transport layer provides to an application. Examples include confidentiality, reliable delivery, ordered delivery, and message-versus-stream orientation.

Transport Service: a set of Transport Features, without an association to any given framing protocol, that provides functionality to an application.

Transport Services system: a software component that exposes an interface to different Transport Services to an application.

Transport Protocol: an implementation that provides one or more different Transport Services using a specific framing and header format on the wire. A Transport Protocol services an application, whether directly or in conjunction with a security protocol.

Application: an entity that uses a transport protocol for end-to-end delivery of data across the network. This may also be an upper layer protocol or tunnel encapsulation.

Security Protocol: a defined network protocol that implements one or more security features, such as authentication, encryption, key generation, session resumption, and privacy. Security protocols may be used alongside transport protocols, and in combination with other security protocols when appropriate.

Handshake Protocol: a protocol that enables peers to validate each other and to securely establish shared cryptographic context.

Record: framed protocol messages.

Record Protocol: a security protocol that allows data to be divided into manageable blocks and protected using shared cryptographic context.

Session: an ephemeral security association between applications.

Connection: the shared state of two or more endpoints that persists across messages that are transmitted between these endpoints. A connection is a transient participant of a session, and a session generally lasts between connection instances.

Peer: an endpoint application party to a session.

Client: the peer responsible for initiating a session.

Server: the peer responsible for responding to a session initiation.

3. Transport Security Protocol Descriptions

This section contains brief transport and security descriptions of various security protocols currently used to protect data being sent over a network. These protocols are grouped based on where in the protocol stack they are implemented, which influences which parts of a packet they protect: Generic application payload, application payload for specific application-layer protocols, both application payload and transport headers, or entire IP packets.

Note that not all security protocols can be easily categorized, e.g., as some protocols can be used in different ways or in combination with other protocols. One major reason for this is that channel security protocols often consist of two components:

- A handshake protocol, which is responsible for negotiating parameters, authenticating the endpoints, and establishing shared keys.
- A record protocol, which is used to encrypt traffic using keys and parameters provided by the handshake protocol.

For some protocols, such as tcpcrypt, these two components are tightly integrated. In contrast, for IPsec, these components are implemented in separate protocols: AH and the Encapsulating Security Payload (ESP) are record protocols, which can use keys supplied by the handshake protocol Internet Key Exchange Protocol Version 2 (IKEv2), by other handshake protocols, or by manual configuration. Moreover, some protocols can be used in different ways: While the base TLS protocol as defined in [RFC8446] has an integrated handshake and record protocol, TLS or DTLS can also be used to negotiate keys for other protocols, as in DTLS-SRTP, or the handshake protocol can be used with a separate record layer, as in QUIC [QUIC-TRANSPORT].

3.1. Application Payload Security Protocols

The following protocols provide security that protects application payloads sent over a transport. They do not specifically protect any headers used for transport-layer functionality.

3.1.1. TLS

TLS (Transport Layer Security) [RFC8446] is a common protocol used to establish a secure session between two endpoints. Communication over this session prevents "eavesdropping, tampering, and message forgery." TLS consists of a tightly coupled handshake and record protocol. The handshake protocol is used to authenticate peers, negotiate protocol options such as cryptographic algorithms, and derive session-specific keying material. The record protocol is used to marshal and, once the handshake has sufficiently progressed, encrypt data from one peer to the other. This data may contain handshake messages or raw application data.

3.1.2. DTLS

DTLS (Datagram Transport Layer Security) [RFC6347] [DTLS-1.3] is based on TLS, but differs in that it is designed to run over unreliable datagram protocols like UDP instead of TCP. DTLS modifies the protocol to make sure it can still provide equivalent security guarantees to TLS with the exception of order protection/non-replayability. DTLS was designed to be as similar to TLS as possible, so this document assumes that all properties from TLS are carried over except where specified.

3.2. Application-Specific Security Protocols

The following protocols provide application-specific security by protecting application payloads used for specific use cases. Unlike the protocols above, these are not intended for generic application use.

3.2.1. Secure RTP

Secure RTP (SRTP) is a profile for RTP that provides confidentiality, message authentication, and replay protection for RTP data packets and RTP control protocol (RTCP) packets [RFC3711]. SRTP provides a record layer only, and requires a separate handshake protocol to provide key agreement and identity management.

The commonly used handshake protocol for SRTP is DTLS, in the form of DTLS-SRTP [RFC5764]. This is an extension to DTLS that negotiates the use of SRTP as the record layer and describes how to export keys for use with SRTP.

ZRTP [RFC6189] is an alternative key agreement and identity management protocol for SRTP. ZRTP Key agreement is performed using a Diffie-Hellman key exchange that runs on the media path. This generates a shared secret that is then used to generate the master key and salt for SRTP.

3.3. Transport-Layer Security Protocols

The following security protocols provide protection for both application payloads and headers that are used for Transport Services.

3.3.1. IETF QUIC

QUIC is a new standards-track transport protocol that runs over UDP, loosely based on Google's original proprietary gQUIC protocol [QUIC-TRANSPORT] (See Section 3.3.2 for more details). The QUIC transport layer itself provides support for data confidentiality and integrity. This requires keys to be derived with a separate handshake protocol. A mapping for QUIC of TLS 1.3 [QUIC-TLS] has been specified to provide this handshake.

3.3.2. Google QUIC

Google QUIC (gQUIC) is a UDP-based multiplexed streaming protocol designed and deployed by Google following experience from deploying SPDY, the proprietary predecessor to HTTP/2. gQUIC was originally known as "QUIC"; this document uses gQUIC to unambiguously distinguish it from the standards-track IETF QUIC. The proprietary technical forebear of IETF QUIC, gQUIC was originally designed with tightly integrated security and application data transport protocols.

3.3.3. tcpcrypt

Tcpcrypt [RFC8548] is a lightweight extension to the TCP protocol for opportunistic encryption. Applications may use tcpcrypt's unique session ID for further application-level authentication. Absent this authentication, tcpcrypt is vulnerable to active attacks.

3.3.4. MinimaLT

MinimaLT [MinimaLT] is a UDP-based transport security protocol designed to offer confidentiality, mutual authentication, DoS prevention, and connection mobility. One major goal of the protocol is to leverage existing protocols to obtain server-side configuration information used to more quickly bootstrap a connection. MinimaLT uses a variant of TCP's congestion control algorithm.

3.3.5. CurveCP

CurveCP [CurveCP] is a UDP-based transport security that, unlike many other security protocols, is based entirely upon public key algorithms. CurveCP provides its own reliability for application data as part of its protocol.

3.4. Packet Security Protocols

The following protocols provide protection for IP packets. These are generally used as tunnels, such as for Virtual Private Networks (VPNs). Often, applications will not interact directly with these protocols. However, applications that implement tunnels will interact directly with these protocols.

3.4.1. IPsec

IKEv2 [RFC7296] and ESP [RFC4303] together form the modern IPsec protocol suite that encrypts and authenticates IP packets, either for creating tunnels (tunnel-mode) or for direct transport connections (transport-mode). This suite of protocols separates out the key generation protocol (IKEv2) from the transport encryption protocol (ESP). Each protocol can be used independently, but this document considers them together, since that is the most common pattern.

3.4.2. WireGuard

WireGuard [WireGuard] is an IP-layer protocol designed as an alternative to IPsec for certain use cases. It uses UDP to encapsulate IP datagrams between peers. Unlike most transport security protocols, which rely on Public Key Infrastructure (PKI) for peer authentication, WireGuard

authenticates peers using pre-shared public keys delivered out of band, each of which is bound to one or more IP addresses. Moreover, as a protocol suited for VPNs, WireGuard offers no extensibility, negotiation, or cryptographic agility.

3.4.3. OpenVPN

OpenVPN [OpenVPN] is a commonly used protocol designed as an alternative to IPsec. A major goal of this protocol is to provide a VPN that is simple to configure and works over a variety of transports. OpenVPN encapsulates either IP packets or Ethernet frames within a secure tunnel and can run over either UDP or TCP. For key establishment, OpenVPN can either use TLS as a handshake protocol or use pre-shared keys.

4. Transport Dependencies

Across the different security protocols listed above, the primary dependency on transport protocols is the presentation of data: either an unbounded stream of bytes, or framed messages. Within protocols that rely on the transport for message framing, most are built to run over transports that inherently provide framing, like UDP, but some also define how their messages can be framed over byte-stream transports.

4.1. Reliable Byte-Stream Transports

The following protocols all depend upon running on a transport protocol that provides a reliable, in-order stream of bytes. This is typically TCP.

Application Payload Security Protocols:

- TLS

Transport-Layer Security Protocols:

- tcpcrypt

4.2. Unreliable Datagram Transports

The following protocols all depend on the transport protocol to provide message framing to encapsulate their data. These protocols are built to run using UDP, and thus do not have any requirement for reliability. Running these protocols over a protocol that does provide reliability will not break functionality but may lead to multiple layers of reliability if the security protocol is encapsulating other transport protocol traffic.

Application Payload Security Protocols:

- DTLS
- ZRTP
- SRTP

Transport-Layer Security Protocols:

- QUIC
- MinimaLT
- CurveCP

Packet Security Protocols:

- IPsec
- WireGuard
- OpenVPN

4.2.1. Datagram Protocols with Defined Byte-Stream Mappings

Of the protocols listed above that depend on the transport for message framing, some do have well-defined mappings for sending their messages over byte-stream transports like TCP.

Application Payload Security Protocols:

- DTLS when used as a handshake protocol for SRTP [RFC7850]
- ZRTP [RFC6189]
- SRTP [RFC4571][RFC3711]

Packet Security Protocols:

- IPsec [RFC8229]

4.3. Transport-Specific Dependencies

One protocol surveyed, tcpcrypt, has a direct dependency on a feature in the transport that is needed for its functionality. Specifically, tcpcrypt is designed to run on top of TCP and uses the TCP Encryption Negotiation Option (TCP-ENO) [RFC8547] to negotiate its protocol support.

QUIC, CurveCP, and MinimaLT provide both transport functionality and security functionality. They depend on running over a framed protocol like UDP, but they add their own layers of reliability and other Transport Services. Thus, an application that uses one of these protocols cannot decouple the security from transport functionality.

5. Application Interface

This section describes the interface exposed by the security protocols described above. We partition these interfaces into pre-connection (configuration), connection, and post-connection interfaces, following conventions in [TAPS-INTERFACE] and [TAPS-ARCH].

Note that not all protocols support each interface. The table in Section 5.4 summarizes which protocol exposes which of the interfaces. In the following sections, we provide abbreviations of the interface names to use in the summary table.

5.1. Pre-connection Interfaces

Configuration interfaces are used to configure the security protocols before a handshake begins or keys are negotiated.

Identities and Private Keys (IPK): The application can provide its identity, credentials (e.g., certificates), and private keys, or mechanisms to access these, to the security protocol to use during handshakes.

- TLS
- DTLS
- ZRTP
- QUIC
- MinimaLT
- CurveCP
- IPsec
- WireGuard
- OpenVPN

Supported Algorithms (Key Exchange, Signatures, and Ciphersuites) (ALG): The application can choose the algorithms that are supported for key exchange, signatures, and ciphersuites.

- TLS
- DTLS
- ZRTP
- QUIC
- tcpcrypt
- MinimaLT
- IPsec
- OpenVPN

Extensions (EXT): The application enables or configures extensions that are to be negotiated by the security protocol, such as Application-Layer Protocol Negotiation (ALPN) [RFC7301].

- TLS
- DTLS
- QUIC

Session Cache Management (CM): The application provides the ability to save and retrieve session state (such as tickets, keying material, and server parameters) that may be used to resume the security session.

- TLS

- DTLS
- ZRTP
- QUIC
- tcpcrypt
- MinimaLT

Authentication Delegation (AD): The application provides access to a separate module that will provide authentication, using the Extensible Authentication Protocol (EAP) [RFC3748] for example.

- IPsec
- tcpcrypt

Pre-Shared Key Import (PSKI): Either the handshake protocol or the application directly can supply pre-shared keys for use in encrypting (and authenticating) communication with a peer.

- TLS
- DTLS
- ZRTP
- QUIC
- tcpcrypt
- MinimaLT
- IPsec
- WireGuard
- OpenVPN

5.2. Connection Interfaces

Identity Validation (IV): During a handshake, the security protocol will conduct identity validation of the peer. This can offload validation or occur transparently to the application.

- TLS
- DTLS
- ZRTP
- QUIC
- MinimaLT
- CurveCP
- IPsec
- WireGuard
- OpenVPN

Source Address Validation (SAV): The handshake protocol may interact with the transport protocol or application to validate the address of the remote peer that has sent data. This involves sending a cookie exchange to avoid DoS attacks. (This list omits protocols that depend on TCP and therefore implicitly perform SAV.)

- DTLS
- QUIC
- IPsec
- WireGuard

5.3. Post-connection Interfaces

Connection Termination (CT): The security protocol may be instructed to tear down its connection and session information. This is needed by some protocols, e.g., to prevent application data truncation attacks in which an attacker terminates an underlying insecure connection-oriented protocol to terminate the session.

- TLS
- DTLS
- ZRTP
- QUIC
- tcpcrypt
- MinimaLT
- IPsec
- OpenVPN

Key Update (KU): The handshake protocol may be instructed to update its keying material, either by the application directly or by the record protocol sending a key expiration event.

- TLS
- DTLS
- QUIC
- tcpcrypt
- MinimaLT
- IPsec

Shared Secret Key Export (SSKE): The handshake protocol may provide an interface for producing shared secrets for application-specific uses.

- TLS
- DTLS
- tcpcrypt
- IPsec

- OpenVPN
- MinimaLT

Key Expiration (KE): The record protocol can signal that its keys are expiring due to reaching a time-based deadline or a use-based deadline (number of bytes that have been encrypted with the key). This interaction is often limited to signaling between the record layer and the handshake layer.

- IPsec

Mobility Events (ME): The record protocol can be signaled that it is being migrated to another transport or interface due to connection mobility, which may reset address and state validation and induce state changes such as use of a new Connection Identifier (CID).

- DTLS (version 1.3 only [DTLS-1.3])
- QUIC
- MinimaLT
- CurveCP
- IPsec [RFC4555]
- WireGuard

5.4. Summary of Interfaces Exposed by Protocols

The following table summarizes which protocol exposes which interface.

Protocol	IPK	ALG	EXT	CM	AD	PSKI	IV	SAV	CT	KU	SSKE	KE	ME
TLS	x	x	x	x		x	x		x	x	x		
DTLS	x	x	x	x		x	x	x	x	x	x		x
ZRTP	x	x		x		x	x		x				
QUIC	x	x	x	x		x	x	x	x	x			x
tcpcrypt		x		x	x	x			x	x	x		
MinimaLT	x	x		x		x	x		x	x	x		x
CurveCP	x						x						x
IPsec	x	x			x	x	x	x	x	x	x	x	x
WireGuard	x					x	x	x					x
OpenVPN	x	x				x	x		x		x		

Table 1

x = Interface is exposed
(blank) = Interface is not exposed

6. IANA Considerations

This document has no IANA actions.

7. Security Considerations

This document summarizes existing transport security protocols and their interfaces. It does not propose changes to or recommend usage of reference protocols. Moreover, no claims of security and privacy properties beyond those guaranteed by the protocols discussed are made. For example, metadata leakage via timing side channels and traffic analysis may compromise any protocol discussed in this survey. Applications using Security Interfaces should take such limitations into consideration when using a particular protocol implementation.

8. Privacy Considerations

Analysis of how features improve or degrade privacy is intentionally omitted from this survey. All security protocols surveyed generally improve privacy by using encryption to reduce information leakage. However, varying amounts of metadata remain in the clear across each protocol. For example, client and server certificates are sent in cleartext in TLS 1.2 [RFC5246], whereas they are encrypted in TLS 1.3 [RFC8446]. A survey of privacy features, or lack thereof, for various security protocols could be addressed in a separate document.

9. Informative References

[ALTS] Ghali, C., Stubblefield, A., Knapp, E., Li, J., Schmidt, B., and J. Boeuf, "Application Layer Transport Security", <https://cloud.google.com/security/encryption-in-transit/application-layer-transport-security/>.

[CurveCP] Bernstein, D., "CurveCP: Usable security for the Internet", <https://curvecp.org/>.

[DTLS-1.3] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-dtls13-38, 29 May 2020, <https://tools.ietf.org/html/draft-ietf-tls-dtls13-38>.

[MinimaLT] Petullo, W., Zhang, X., Solworth, J., Bernstein, D., and T. Lange, "MinimaLT: minimal-latency networking through better security", DOI 10.1145/2508859.2516737, <https://dl.acm.org/citation.cfm?id=2516737>.

[OpenVPN] OpenVPN, "OpenVPN cryptographic layer", <https://openvpn.net/community-resources/openvpn-cryptographic-layer/>.

[QUIC-TLS] Thomson, M. and S. Turner, "Using TLS to Secure QUIC", Work in Progress, Internet-Draft, draft-ietf-quic-tls-31, 24 September 2020, <https://tools.ietf.org/html/draft-ietf-quic-tls-31>.

[QUIC-TRANSPORT] Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport", Work in Progress, Internet-Draft, draft-ietf-quic-transport-31, 24 September 2020, <https://tools.ietf.org/html/draft-ietf-quic-transport-31>.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, DOI 10.17487/RFC2385, August 1998, <https://www.rfc-editor.org/info/rfc2385>.

[RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, DOI 10.17487/RFC2890, September 2000, <https://www.rfc-editor.org/info/rfc2890>.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, DOI 10.17487/RFC3711, March 2004, <https://www.rfc-editor.org/info/rfc3711>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, <https://www.rfc-editor.org/info/rfc3748>.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, January 2006, <https://www.rfc-editor.org/info/rfc4253>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, DOI 10.17487/RFC4555, June 2006, <https://www.rfc-editor.org/info/rfc4555>.

[RFC4571] Lazzaro, J., "Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport", RFC 4571, DOI 10.17487/RFC4571, July 2006, <https://www.rfc-editor.org/info/rfc4571>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5641] McGill, N. and C. Pignataro, "Layer 2 Tunneling Protocol Version 3 (L2TPv3) Extended Circuit Status Values", RFC 5641, DOI 10.17487/RFC5641, August 2009, <https://www.rfc-editor.org/info/rfc5641>.

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, DOI 10.17487/RFC5764, May 2010, <https://www.rfc-editor.org/info/rfc5764>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[RFC6189] Zimmermann, P., Johnston, A., Ed., and J. Callas, "ZRTP: Media Path Key Agreement for Unicast Secure RTP", RFC 6189, DOI 10.17487/RFC6189, April 2011, <https://www.rfc-editor.org/info/rfc6189>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/info/rfc7301>.

[RFC7850] Nandakumar, S., "Registering Values of the SDP 'proto' Field for Transporting RTP Media over TCP under Various RTP Profiles", RFC 7850, DOI 10.17487/RFC7850, April 2016, <https://www.rfc-editor.org/info/rfc7850>.

[RFC8095] Fairhurst, G., Ed., Trammell, B., Ed., and M. Kuehlewind, Ed., "Services Provided by IETF Transport Protocols and Congestion Control Mechanisms", RFC 8095, DOI 10.17487/RFC8095, March 2017, <https://www.rfc-editor.org/info/rfc8095>.

[RFC8229] Pauly, T., Touati, S., and R. Mantha, "TCP Encapsulation of IKE and IPsec Packets", RFC 8229, DOI 10.17487/RFC8229, August 2017, <https://www.rfc-editor.org/info/rfc8229>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8547] Bittau, A., Giffin, D., Handley, M., Mazieres, D., and E. Smith, "TCP-ENO: Encryption Negotiation Option", RFC 8547, DOI 10.17487/RFC8547, May 2019, <https://www.rfc-editor.org/info/rfc8547>.

[RFC8548] Bittau, A., Giffin, D., Handley, M., Mazieres, D., Slack, Q., and E. Smith, "Cryptographic Protection of TCP Streams (tcpcrypt)", RFC 8548, DOI 10.17487/RFC8548, May 2019, <https://www.rfc-editor.org/info/rfc8548>.

[TAPS-ARCH] Pauly, T., Trammell, B., Brunstrom, A., Fairhurst, G., Perkins, C., Tiesel, P. S., and C. A. Wood, "An Architecture for Transport Services", Work in Progress, Internet-Draft, draft-ietf-taps-arch-08, 13 July 2020, <https://tools.ietf.org/html/draft-ietf-taps-arch-08>.

[TAPS-INTERFACE] Trammell, B., Welzl, M., Enghardt, T., Fairhurst, G., Kuehlewind, M., Perkins, C., Tiesel, P. S., Wood, C. A., and T. Pauly, "An Abstract Application Layer Interface to Transport Services", Work in Progress, Internet-Draft, draft-ietf-taps-interface-09, 27 July 2020, <https://tools.ietf.org/html/draft-ietf-taps-interface-09>.

[WireGuard] Donenfeld, J., "WireGuard: Next Generation Kernel Network Tunnel", <https://www.wireguard.com/papers/wireguard.pdf>.

Acknowledgments

The authors would like to thank Bob Bradley, Frederic Jacobs, Mirja Kühlewind, Yannick Sierra, Brian Trammell, and Magnus Westerlund for their input and feedback on this document.

Authors' Addresses

Theresa Enghardt
TU Berlin
Marchstr. 23
10587 Berlin
Germany
Email: ietf@tenghardt.net

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America
Email: tpauly@apple.com

Colin Perkins
University of Glasgow
School of Computing Science
Glasgow
G12 8QQ
United Kingdom
Email: csp@csperkins.org

Kyle Rose
Akamai Technologies, Inc.
150 Broadway
Cambridge, MA 02144
United States of America
Email: krose@krose.org

Christopher A. Wood
Cloudflare
101 Townsend St
San Francisco,
United States of America
Email: caw@heapingbits.net