

# A Survey of Transport Security Protocols

**draft-taps-transport-security**

Tommy Pauly ([tpauly@apple.com](mailto:tpauly@apple.com))

Colin Perkins ([csp@csp Perkins.org](mailto:csp@csp Perkins.org))

Kyle Rose ([krose@krose.org](mailto:krose@krose.org))

Christopher A. Wood ([cawood@apple.com](mailto:cawood@apple.com))

TAPS

IETF 102, July 2018, Montreal

# Updates

- Improve protocol justification text, and sort protocols based on use and impact
- Canonicalization of security feature set
- Interface cleanup

# Security Feature Set

- Forward-secure key establishment
- Cryptographic algorithm negotiation
- Stateful and stateless cross-connection session resumption
- Peer authentication
- Mutual authentication
- Record confidentiality and integrity (partial confidentiality and integrity, too)
- ...

# Mandatory Features

- Segment or datagram encryption and authentication
- Forward-secure key establishment
- Public key (raw- or certificate-based) authentication
- Responder authentication
- Pre-shared key support

# Optional Feature Applicability

**Optional features** are optional, and applicable to some protocols

Protocol	AN	AD	MA	DM	CM	SV	AFN	CX	SC	LHP
TLS	S	S	S	S	U*	M	S	S	S	S
DTLS	S	S	S	S	S	M	S	S	S	S
IETF QUIC	S	S	S	S	S	M	S	S	S	S
IKEv2+ESP	S	S	M	S	S	M	S	S	S	S
SRTP+DTLS	S	S	S	S	U	M	S	S	S	U
tcpcrypt	S	M	U	U**	U*	M	U	U	S	U
WireGuard	U	S	M	S	U	M	U	U	U	S+
MinimalT	U	U	M	S	M	M	U	U	U	S
CurveCP	U	U	S	S	M	M	U	U	U	S

M=Mandatory

S=Supported but not required

U=Unsupported

\*=On TCP; MPTCP would provide this ability

\*\*=TCP provides SYN cookies natively, but these are not cryptographically strong

+ =For transport packets only

Systems wanting to provide cryptographic algorithm negotiation (AN) and mutual authentication (MA) can support protocols in blue

Protocol	AN	AD	MA	DM	CM	SV	AFN	CX	SC	LHP
TLS	S	S	S	S	U*	M	S	S	S	S
DTLS	S	S	S	S	S	M	S	S	S	S
IETF QUIC	S	S	S	S	S	M	S	S	S	S
IKEv2+ESP	S	S	M	S	S	M	S	S	S	S
SRTP+DTLS	S	S	S	S	U	M	S	S	S	U
tcpcrypt	S	M	U	U**	U*	M	U	U	S	U
WireGuard	U	S	M	S	U	M	U	U	U	S+
MinimalT	U	U	M	S	M	M	U	U	U	S
CurveCP	U	U	S	S	M	M	U	U	U	S

M=Mandatory

S=Supported but not required

U=Unsupported

\*=On TCP; MPTCP would provide this ability

\*\*=TCP provides SYN cookies natively, but these are not cryptographically strong

+ =For transport packets only

# Example

Systems which **MUST** provide connection mobility (CM) and session caching and management (SC) should implement protocols in blue

Protocol	AN	AD	MA	DM	CM	SV	AFN	CX	SC	LHP
TLS	S	S	S	S	U*	M	S	S	S	S
DTLS	S	S	S	S	S	M	S	S	S	S
IETF QUIC	S	S	S	S	S	M	S	S	S	S
IKEv2+ESP	S	S	M	S	S	M	S	S	S	S
SRTP+DTLS	S	S	S	S	U	M	S	S	S	U
tcpcrypt	S	M	U	U**	U*	M	U	U	S	U
WireGuard	U	S	M	S	U	M	U	U	U	S+
MinimalT	U	U	M	S	M	M	U	U	U	S
CurveCP	U	U	S	S	M	M	U	U	U	S

M=Mandatory

S=Supported but not required

U=Unsupported

\*=On TCP; MPTCP would provide this ability

\*\*=TCP provides SYN cookies natively, but these are not cryptographically strong

+ =For transport packets only

# Informal Feedback

Remove protocol details that do not affect features or interfaces

- Example: IKEv2 details are irrelevant

# Informal Feedback

Trying to generalize security interfaces for all protocols is **hard**

- Generic and protocol-specific interfaces must be provided.
- Generic ones permit protocols to be added, specific ones permit applications to tune particular protocol behavior (and possibly ossify)

# Informal Feedback

Protocol equivalence **MUST** be based on name, not feature availability

- We cannot (yet) prove security protocol equivalence, so do not attempt to do so
- Implications on TAPS architecture and implementation drafts

# Next Steps

- Formally circulate draft to security area for feedback
- Consider relocating “obscure” protocols, e.g., MinimalT and CurveCP

# QUESTIONS?