Separating Crypto Negotiation and Communication

Mirja Kühlewind (mirja.kuehlewind@tik.ee.ethz.ch)
Tommy Pauly (tpauly@apple.com)
Christopher A. Wood (cwood@apple.com)

OPSEC
IETF 100, November 2017, Singapore
Goals

1. Survey transport security protocols in use today

2. Factor out transport, handshake (control), and record modules of each protocol
Terminology

- **Handshake**: a module that performs a handshake to validate peers and establish a shared cryptographic key.

- **Record**: a module that packages encrypted data in records using a shared cryptographic key.

- **Transport**: a module that sends and receives data (or records).
Separation of Concerns

Transport 

Handshake

Record
Separation of Concerns

- Transport
- Handshake
- Record

- Private key interface or injection
- Endpoint authentication
- Source validation
- Forward-secure key exchange

...
Separation of Concerns

- Record encryption and authentication
- Pre-shared key support
Separation of Concerns

RFC 8095: Services Provided by IETF Transport Protocols and Congestion Control Mechanisms

Record \rightarrow Transport \rightarrow Handshake
QUIC + TLS

Application

read/write

QUIC

handshake ➔
validate addr ➔
ok/error/validate ➔
handshake ➔
validate ➔
export keys ➔
handshake done ➔

TLS

got secret

Packet Protector

get secret

Unreliable Transport (UDP)

read/write

packet ➔
protected packet ➔

secret ➔

Transport Security and Crypto Sep - OPSEC - IETF 100
tcpcrypt

Application

TCP
tcpcrypt

read/write

Transport
Handshake
Record
IKEv2+ESP

Application

IKEv2
- config
- export key
- spawn SA
- rekey
- read/write

ESP
- read/write

Unreliable Delivery (IP)
- read/write
Separation Benefits

• Reducing connection latency
• Protocol flexibility
• Protocol capability negotiation
• Modular software design
Ongoing & Future Work

- Integrate module interface(s) into TAPS minset
- Expand survey of security protocols to ensure adequate interface coverage
- Review by Security Area