Separating Crypto Negotiation and Communication

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

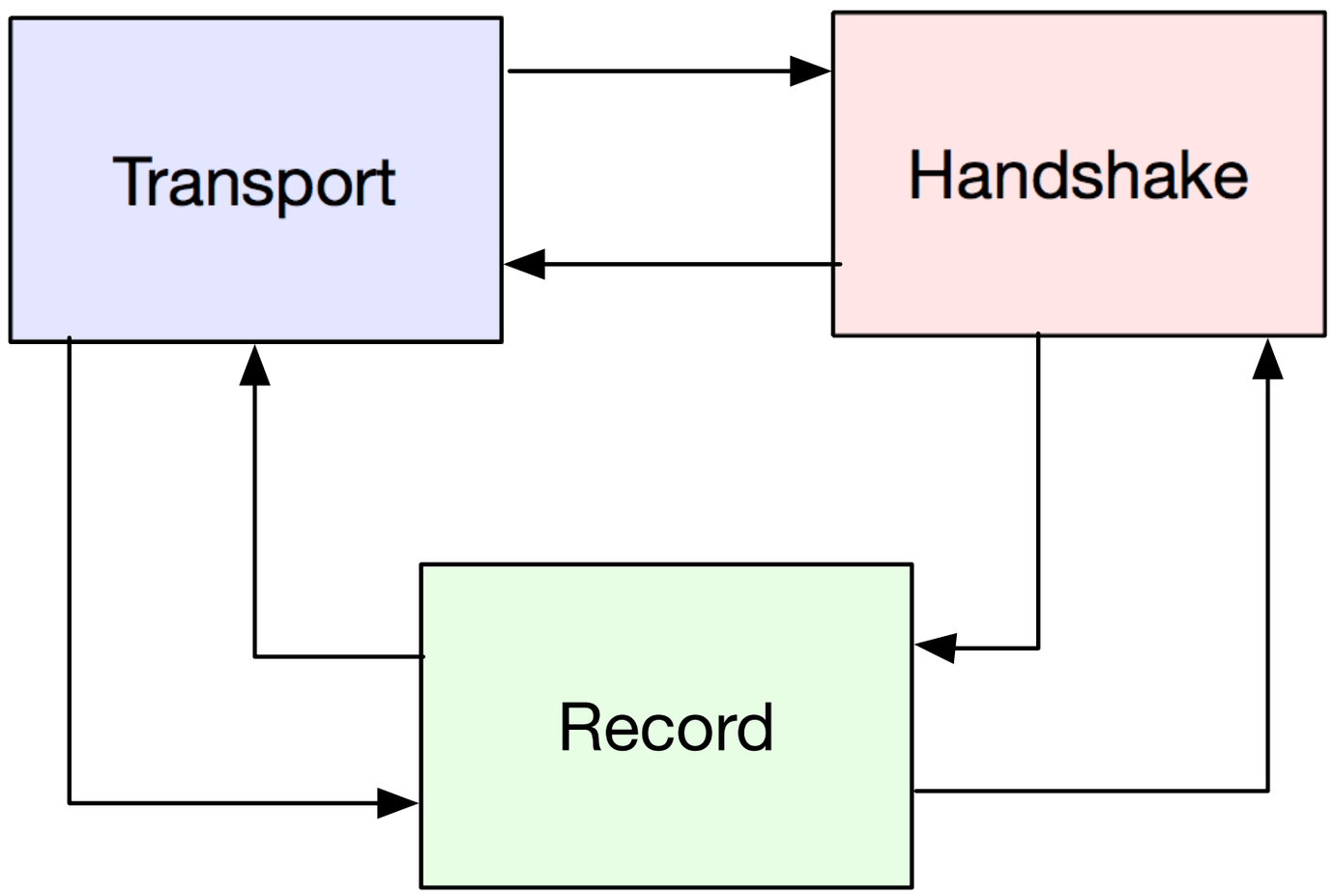
Terminology

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

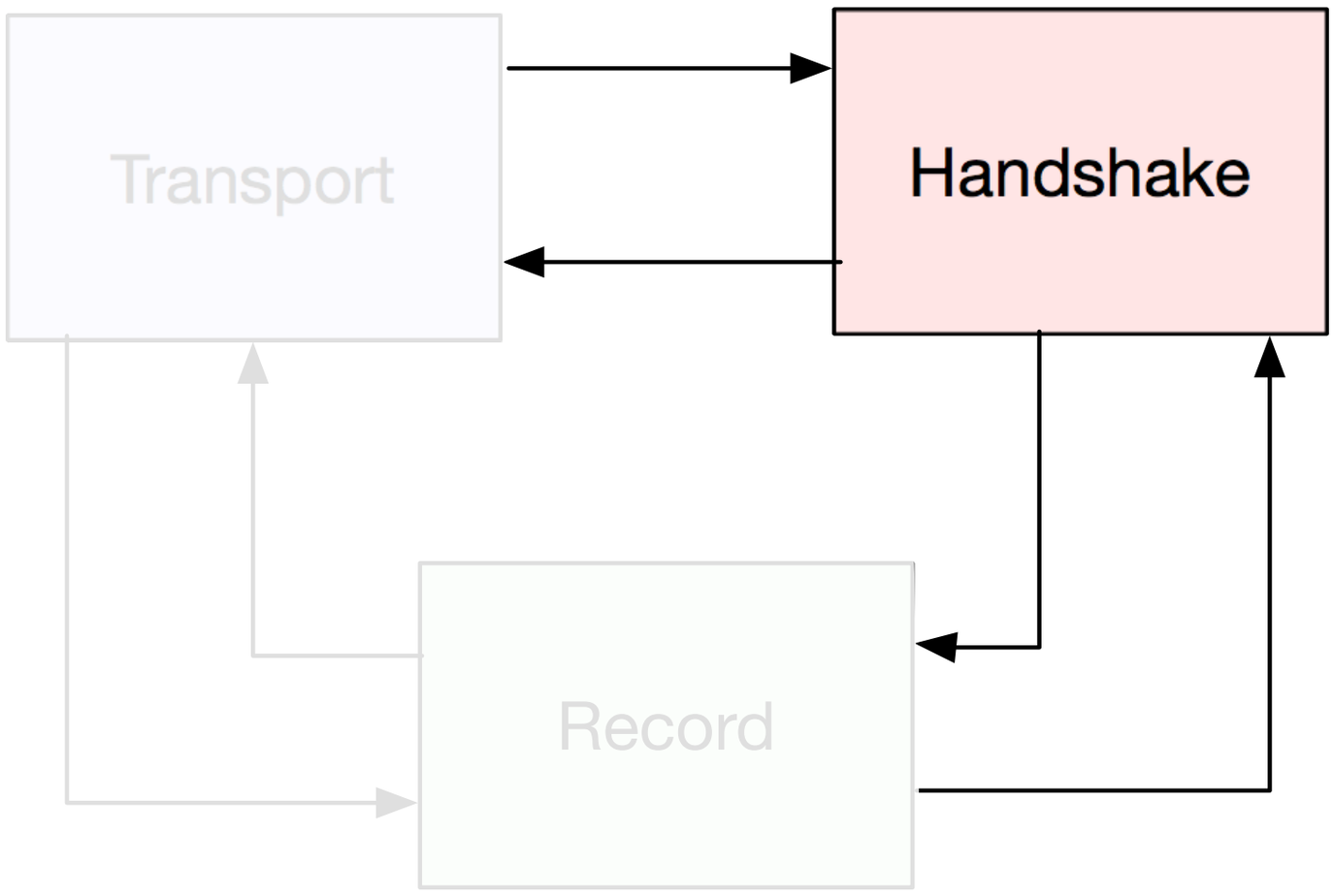
- **Record**: a module that packages encrypted data in records using a shared cryptographic key.

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

Separation of Concerns



Separation of Concerns



Private key interface or injection

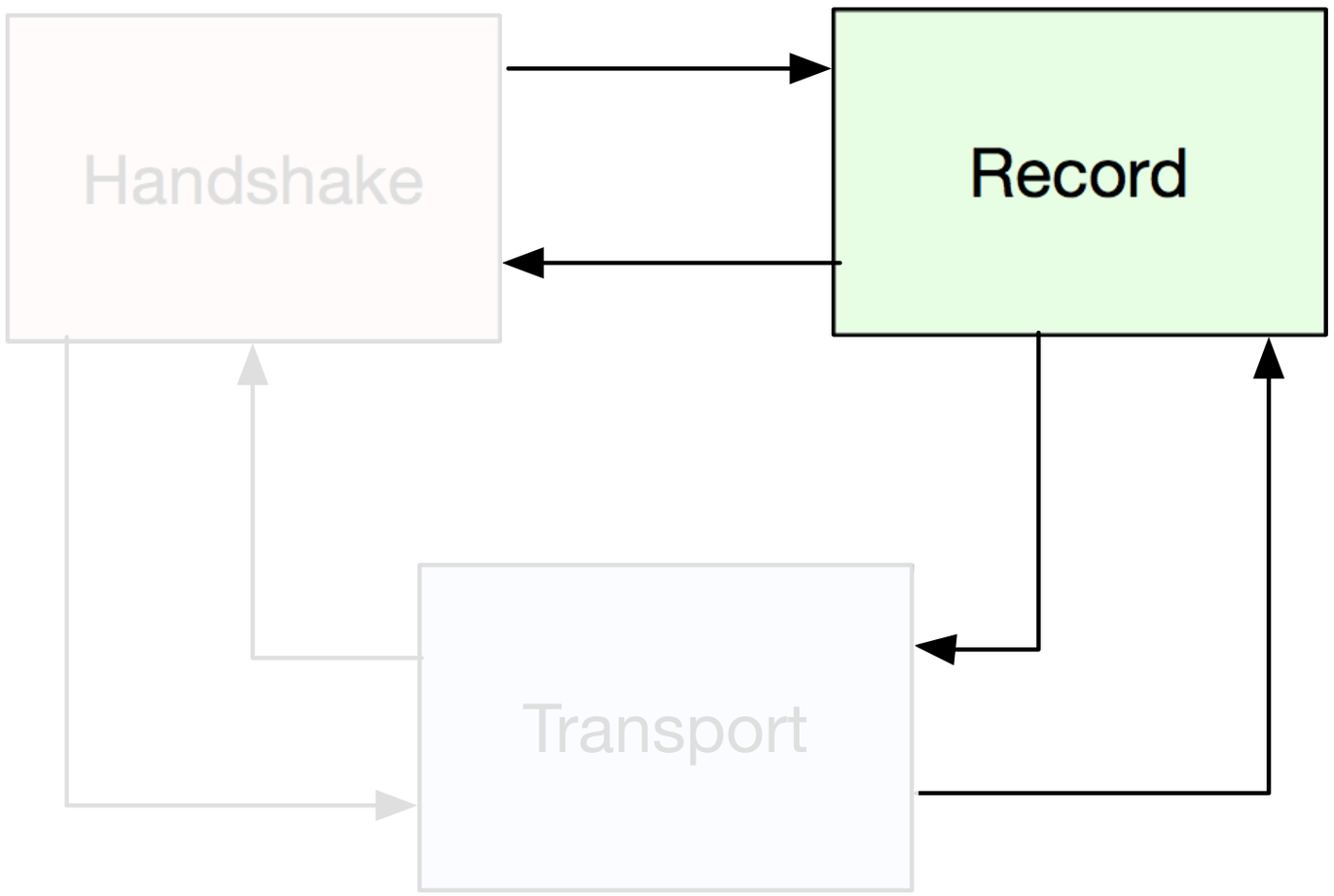
Endpoint authentication

Source validation

Forward-secure key exchange

…

Separation of Concerns

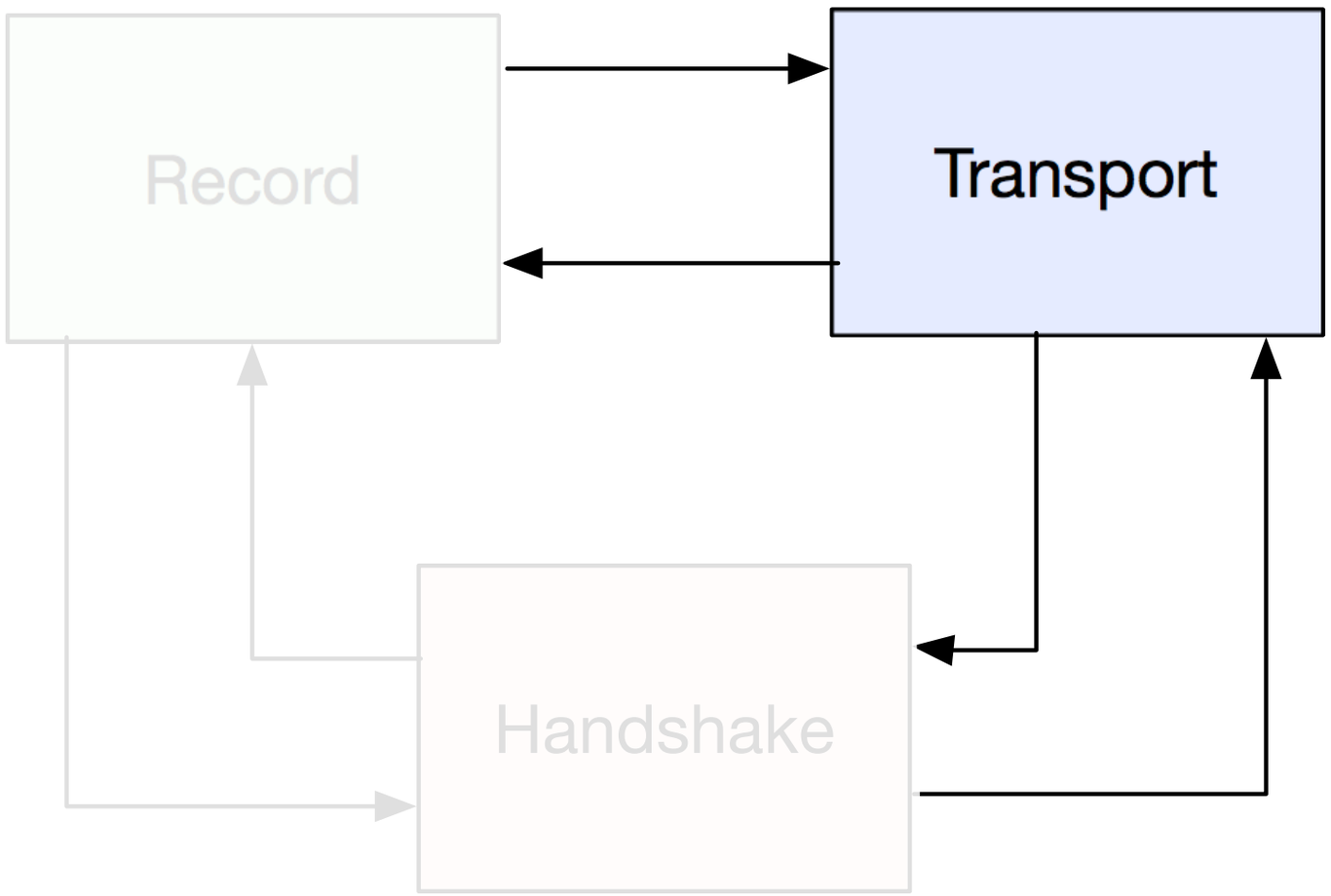


Record encryption and authentication

Pre-shared key support

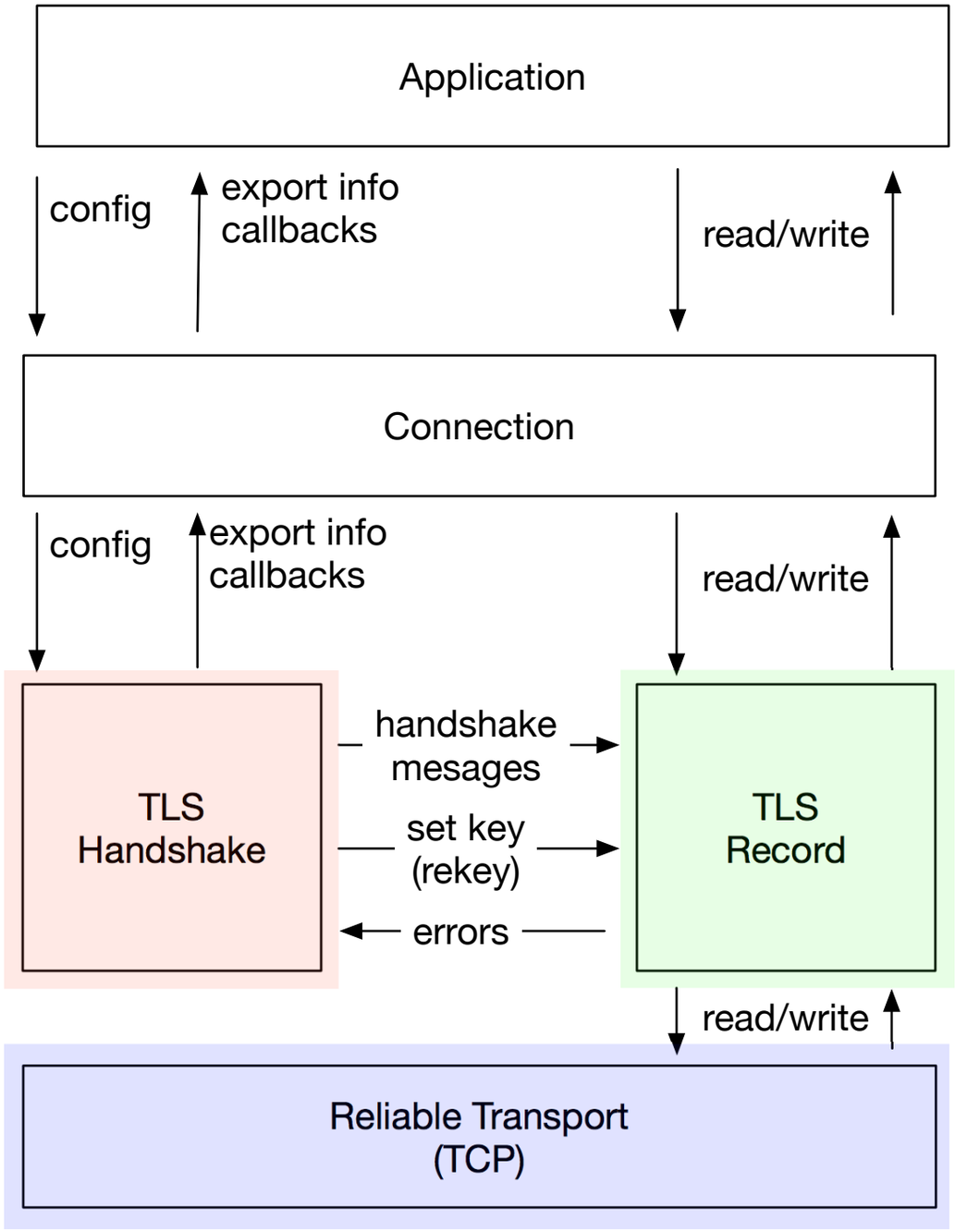
...

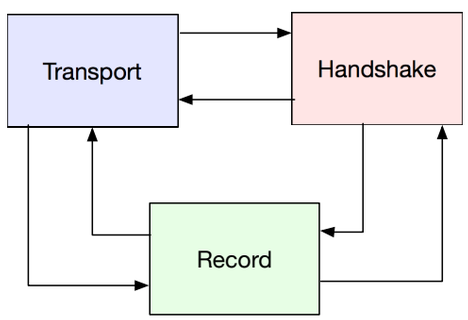
Separation of Concerns



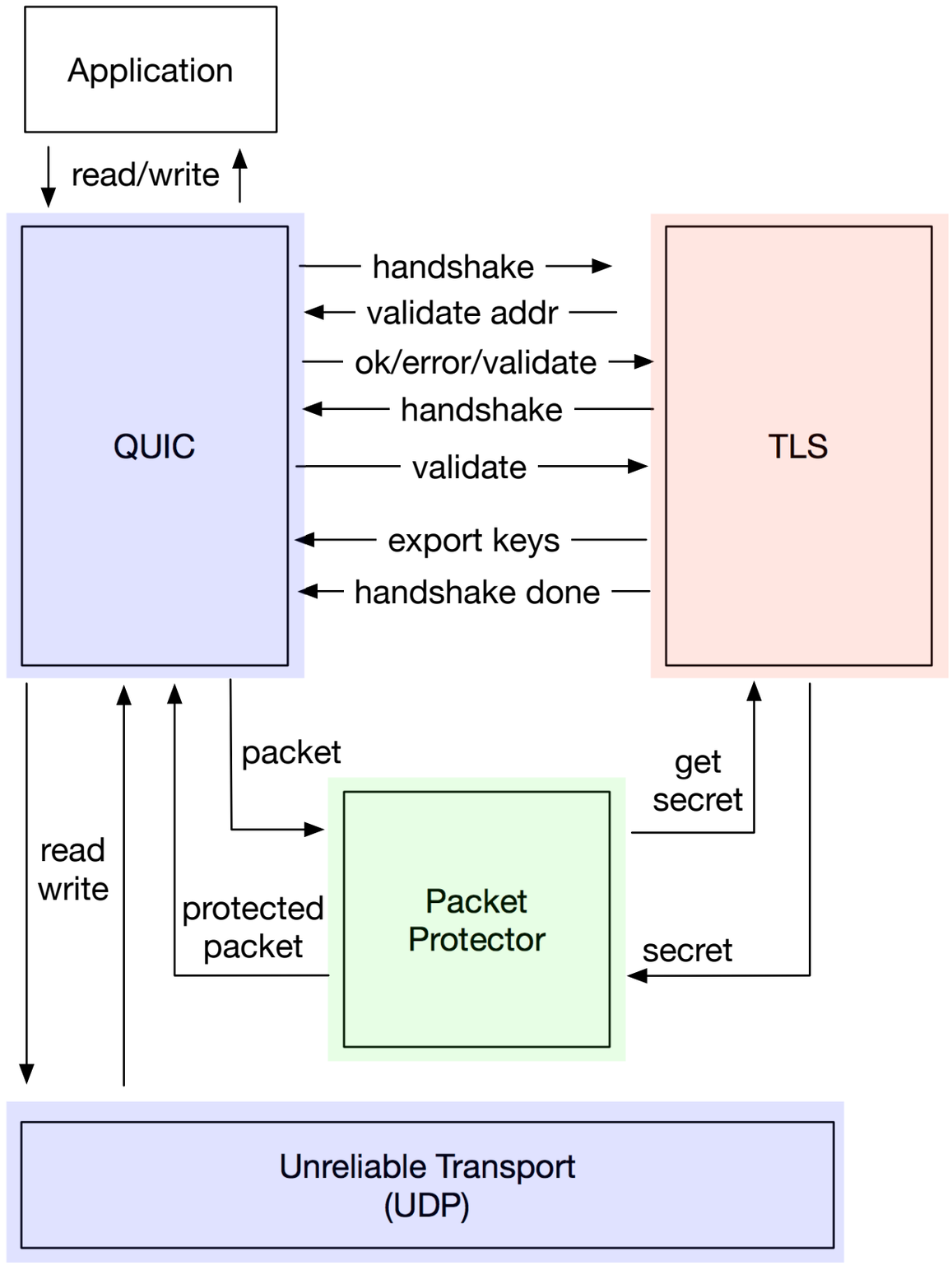
RFC 8095: Services Provided by IETF Transport Protocols and Congestion Control Mechanisms

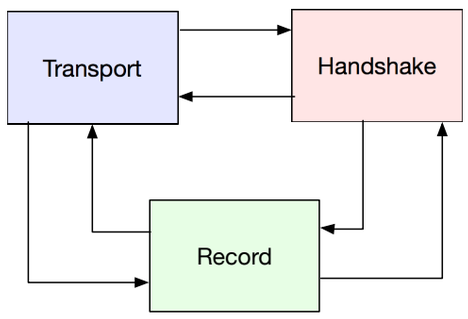
TLS


Application
config
export info
callbacks
read/write
Connection
config
export info
callbacks
read/write
TLS
Handshake
handshake
mesages
set key
(rekey)
errors
TLS
Record
read/write
Reliable Transport
(TCP)

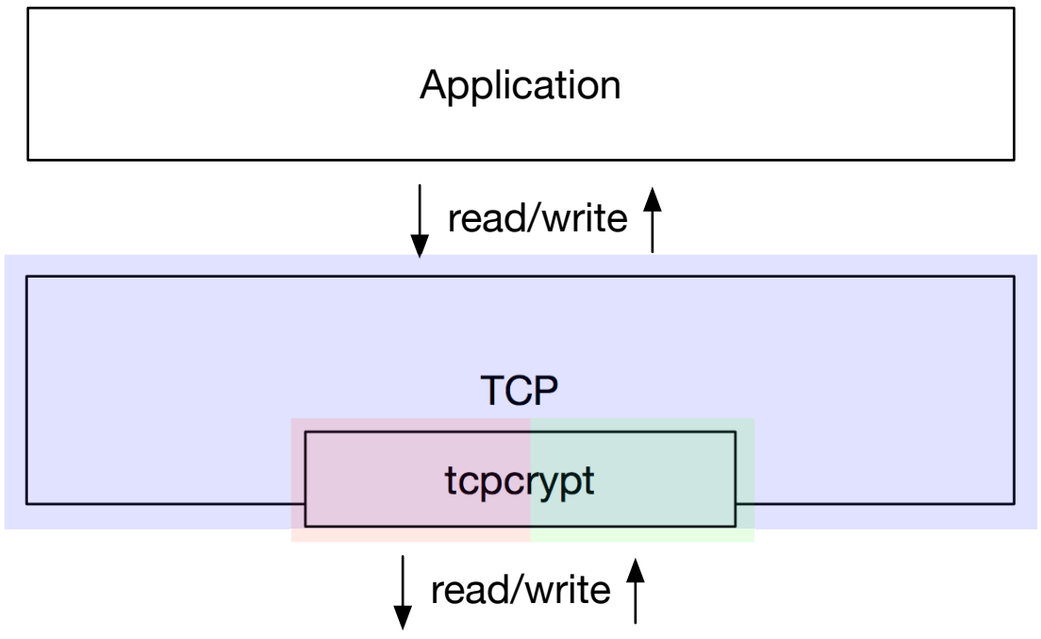

Transport
Handshake
Record

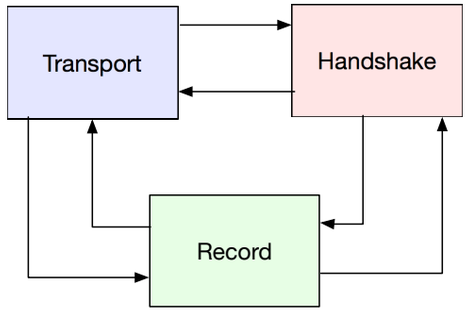
QUIC+TLS


Application
read/write
QUIC
handshake
validate addr
ok/error/validate
handshake
validate
export keys
handshake done
TLS
packet
get secret
read
write
protected packet
Packet Protector
secret
Unreliable Transport (UDP)

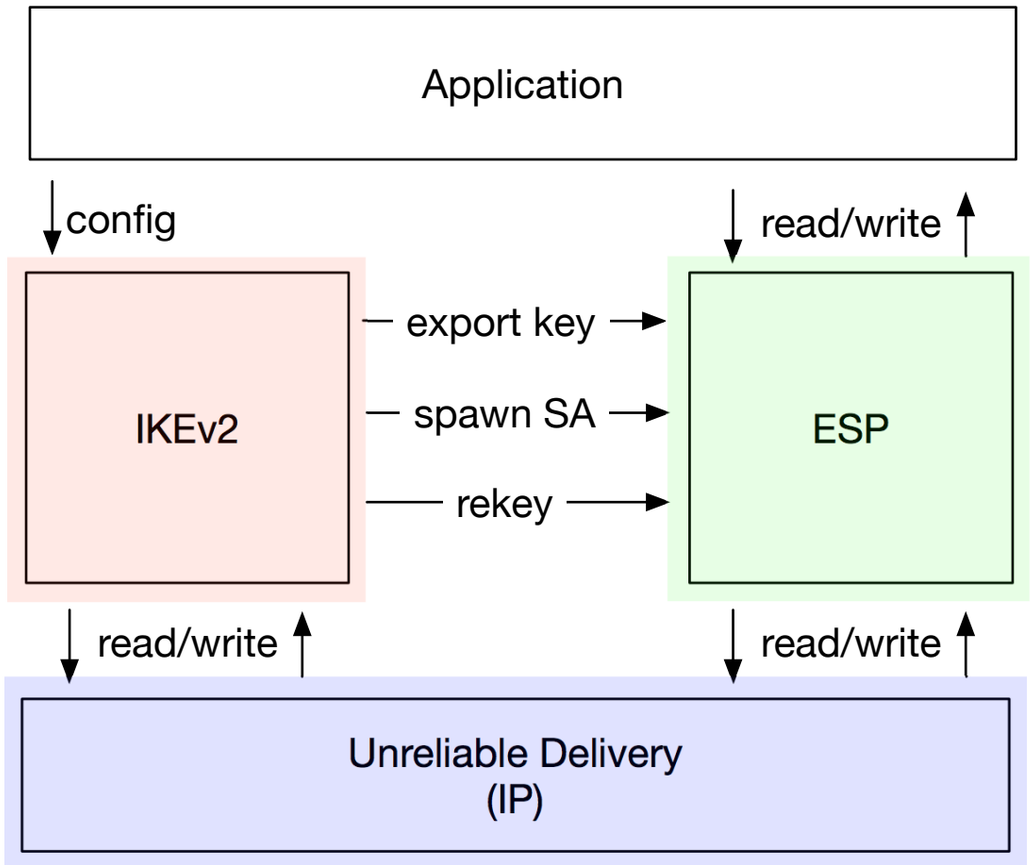

Transport
Handshake
Record

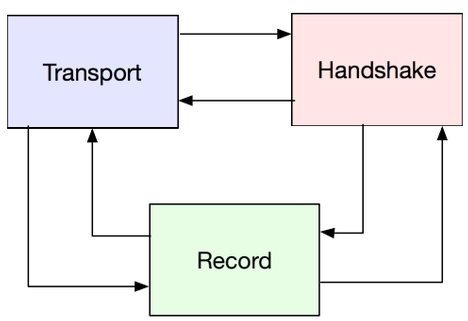
tcpcrypt


Application
read/write
TCP
tcpcrypt
read/write


Transport
Handshake
Record

IKEv2+ESP


Application
config
read/write
export key
spawn SA
rekey
IKEv2
ESP
read/write
read/write
Unreliable Delivery
(IP)


Transport
Handshake
Record

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