IETF Principles for Encrypted Protocols

Sean Turner
sean@sn3rd.com

DISCLAIMERS

- sn3rd

Foundational RFCs

RFC 1984: IAB & IESG Statement on Cryptographic Technology and the Internet

RFC 2804: IETF Policy on Wiretapping

RFC 3552: Guidelines for Writing RFC Text on Security Considerations

RFC 6973: Privacy Considerations for Internet Protocols

RFC 7258: Pervasive Monitoring is an Attack

TLS 1.3 Motivations

ATTACKS GALORE

- Lucky 13
- BEAST
- Crime
- Freak
- Breach
- Logjam
- Poodle
- Drown
- Sweet32
- Triple Handshake

TLS 1.3 Design Goals

Get security researchers involved in the standardization process ASAP. Security analysis and proofs published at NDSS 2016's TRON (TLS Ready Or Not) Workshop.

Security

Privacy

Speed

Dropped Dodgy Algorithms

1 SHA-1

Insufficient Collision Resistance

Deprecated: NIST SP-131A

2 Static RSA/DH Key Exchange

Neither offered Forward Secrecy

3 Stream Ciphers

Insecure

Deprecated: RFC 7465

4 Block Ciphers

Way, way too many attacks

Better Security with Less

The number of ciphers suites:

TLS 1.2 > 100

TLS 1.3 = 5*

Record Payload Algorithms

AEAD-only

Key Establishment Algorithms

(EC)DHE or PSK

Converged

PSK, Session Resumption & Tickets, and 0-RTT

Privacy Features

Forward Secrecy

Forward secrecy is the default.*

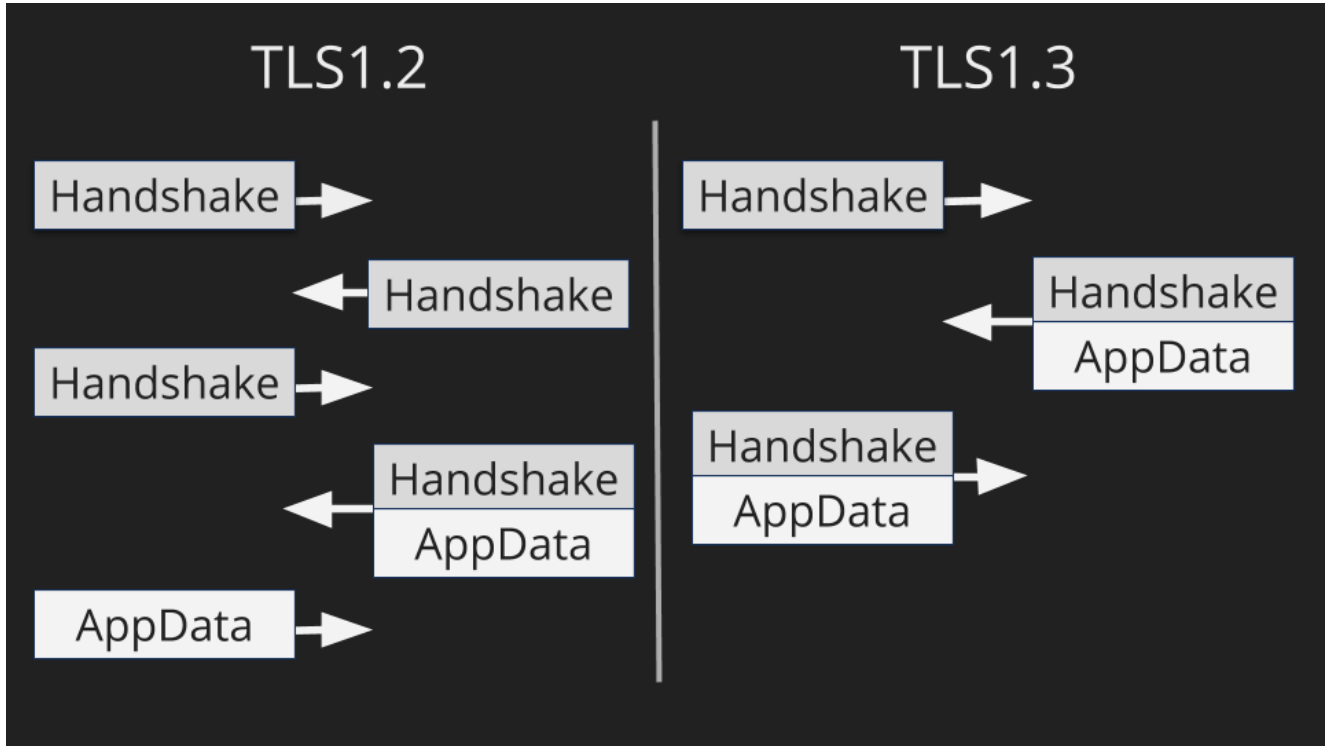
Padding

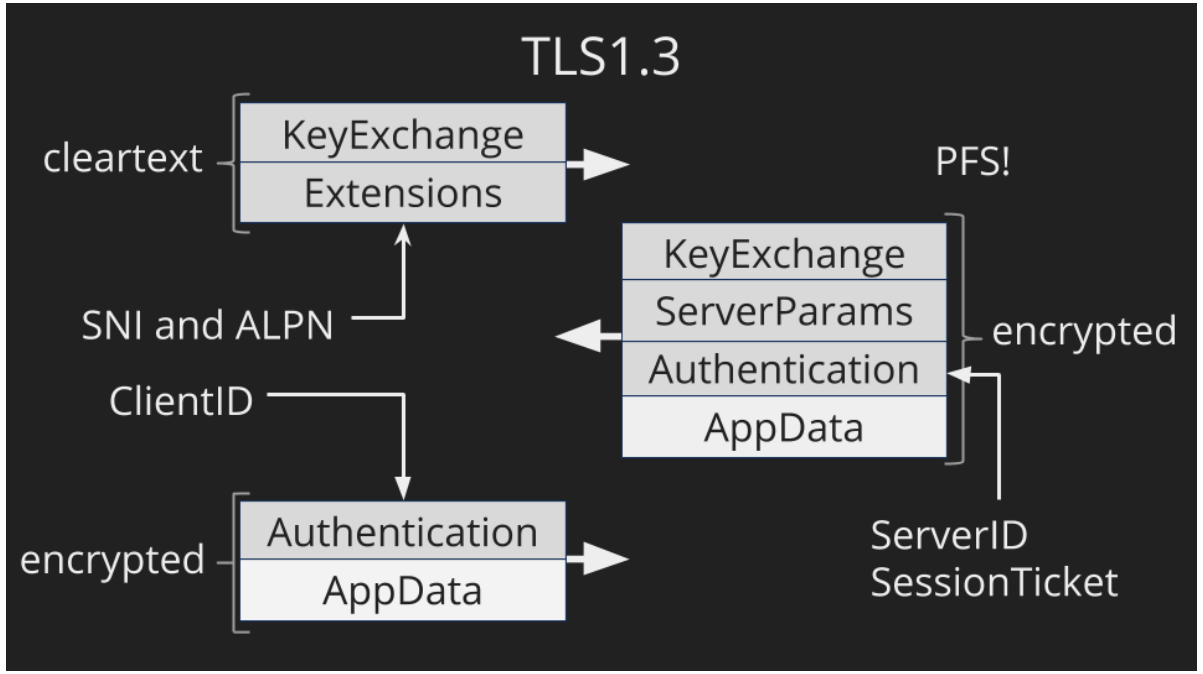
TLSInnerPlainText adds optional support for length hiding.

Stick Out Less

ContentType and Version, which are both unencrypted, are now fixed values rendering them meaningless.

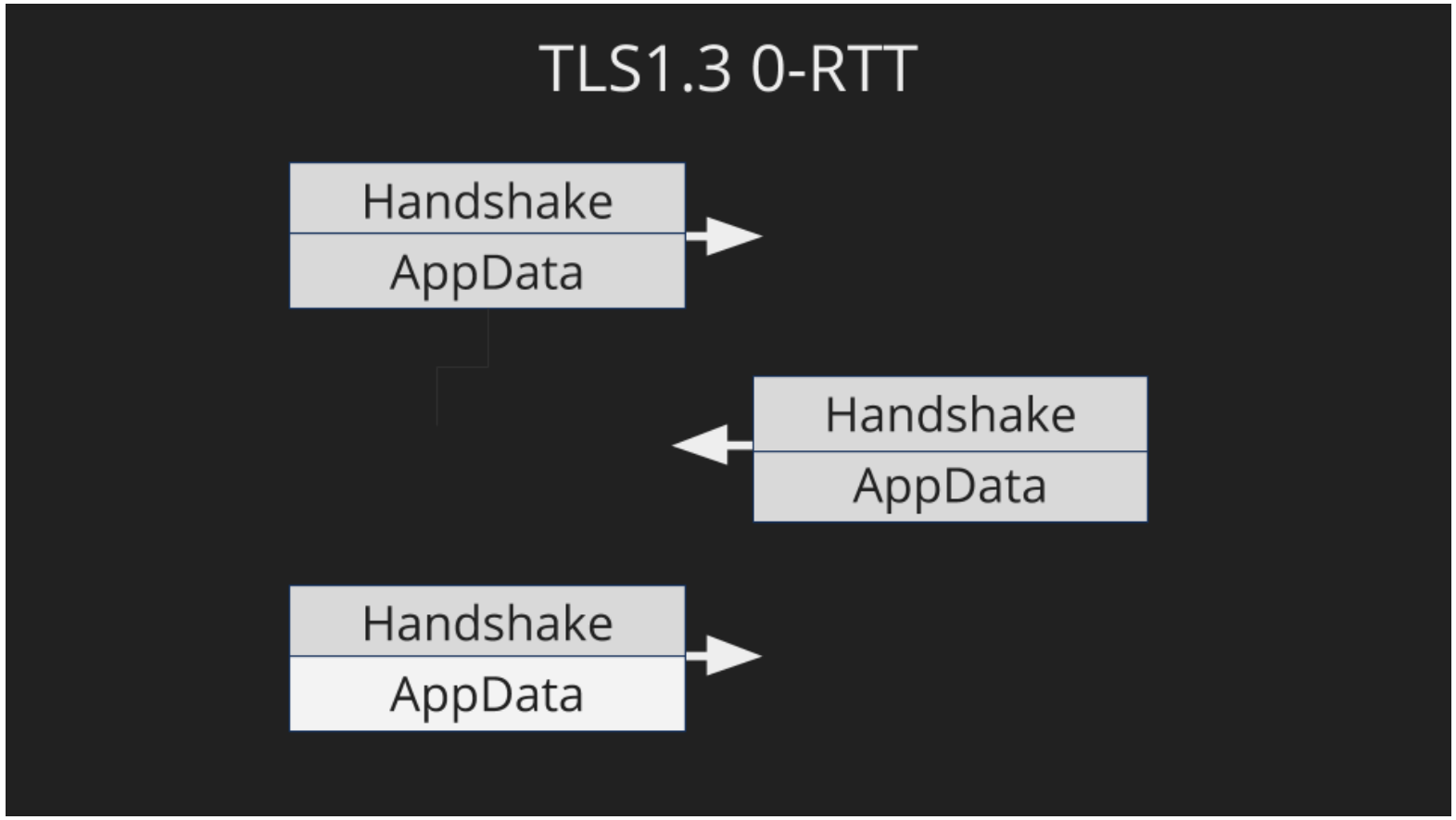
Speed It Up





Encrypt more earlier!

Speed It WAY Up



WARNING: 0-RTT Data is re-playable and not Forward Secure!

What Is Next?

Encrypted Client Hello (formerly Encrypted SNI)

Semi-Static DH Key Exchange

Delegated Credentials

Hybrid Key Exchange

Compact TLS

Questions?