Application Layer TLS draft-friel-tls-atls-00

Friel, Barnes, Pritikin - cisco

Tschofenig – ARM

Baugher - Consultant

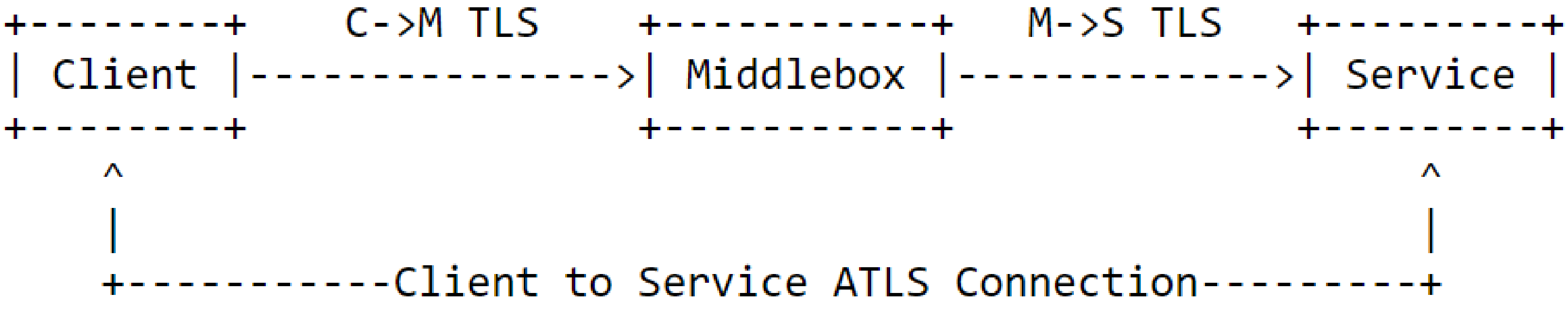
Summary and Goals

- ATLS Summary
  - Establish end-to-end encrypted channel / shared encryption keys between client and server over untrusted transport
  - Achieved by exchanging TLS Handshake Records at the application layer between client and service over untrusted transport
    - Where transport includes gateways, middleboxes; using HTTP, CoAP, Zigbee, etc.
  - Define packaging and content type to explicitly identify ATLS payload to middleboxes
- Goals
  - Based on Monday's reasonably positive* ATLS Lunch Meeting determine if this warrants further investigation and assessment
  - Determine best path forward: Adoption by a WG? New mini-WG?

*Show of hands indicated ~10 people (30%) interested in further investigation
Two primary concerns raised: DKG – future AATLS, AAATLS, etc.; P.McM – HTTP is an unreliable transport substrate

Use Cases – Bootstrapping Devices

- Bootstrapping device that needs to establish trust in network layer TLS middlebox by downloading trust anchors from service

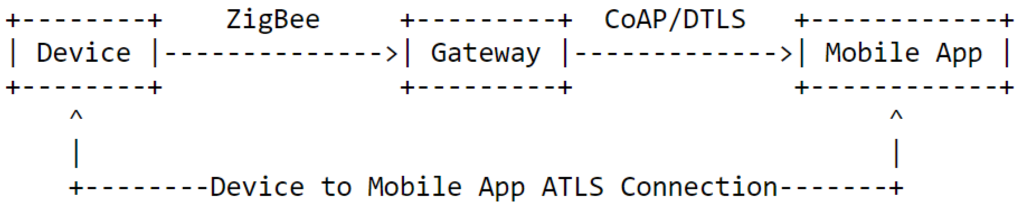


```
+--------+    C->M TLS    +-----------+  M->S TLS    +---------+
| Client |--------------->| Middlebox |------------->| Service |
+--------+                +-----------+              +---------+
    ^                                                     ^
    |                                                     |
    +-----------Client to Service ATLS Connection---------+
```

Figure 1: Bootstrapping Devices

Use Cases – Constrained Devices

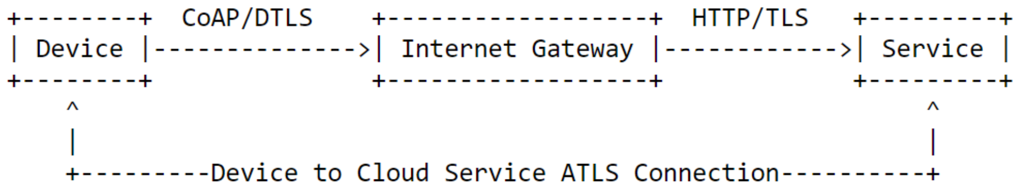
- Constrained device / thing connecting via a gateway to a mobile app where data must be protected from gateway



```
+--------+    ZigBee     +---------+  CoAP/DTLS   +------------+
| Device |-------------->| Gateway |------------->| Mobile App |
+--------+               +---------+              +------------+
    ^                                                   ^
    |                                                   |
    +--------Device to Mobile App ATLS Connection-------+
```

Figure 2: IoT Closed Network Gateway

- Constrained device / thing connecting via an internet gateway to a cloud service where data must be protected from gateway



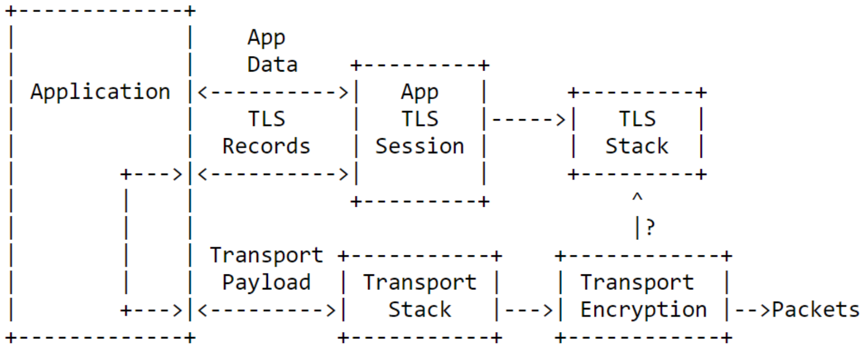
```
+--------+  CoAP/DTLS    +------------------+  HTTP/TLS   +---------+
| Device |------------->| Internet Gateway |------------>| Service |
+--------+              +------------------+             +---------+
    ^                                                         ^
    |                                                         |
    +---------Device to Cloud Service ATLS Connection---------+
```

Figure 3: IoT Internet Gateway

Implementation Options

1. D/TLS Data Records

- Encrypted Data transported inside D/TLS Records

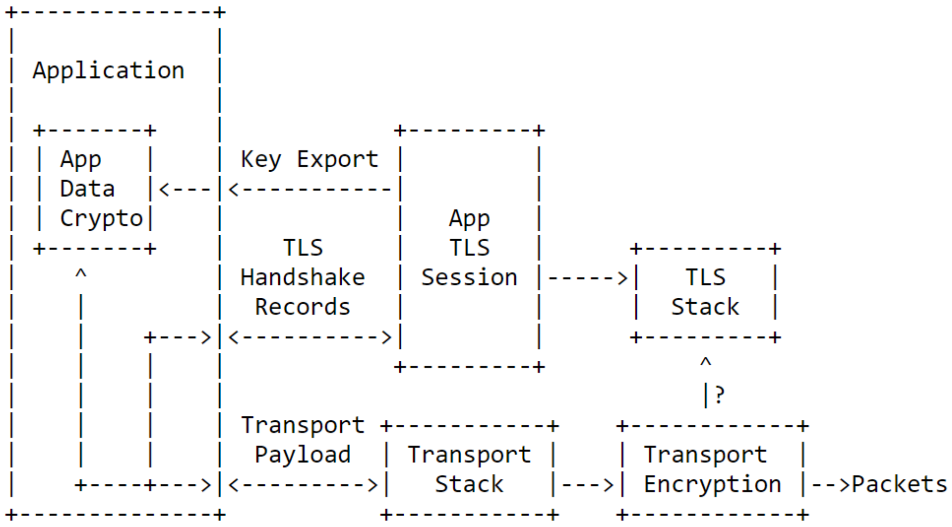


```
+-------------+
|             |    App
|             |    Data   +---------+
| Application |<---------->|   App   |       +---------+
|             |    TLS    |   TLS   |------>|   TLS   |
|             |  Records  | Session |       |  Stack  |
|        +--->|<---------->|         |       +---------+
|        |    |           +---------+            ^
|        |    |                                  |?
|        |    | Transport +-----------+   +------------+
|        |    |  Payload  | Transport |   | Transport  |
|        +--->|<--------->|   Stack   |--->| Encryption |-->Packets
+-------------+           +-----------+   +------------+
```

Figure 5: TLS Stack used for all data encryption

2. Key exporting

- ATLS only used for handshake (2xRTT) and key exporting
- Data encrypted by application using shared keys

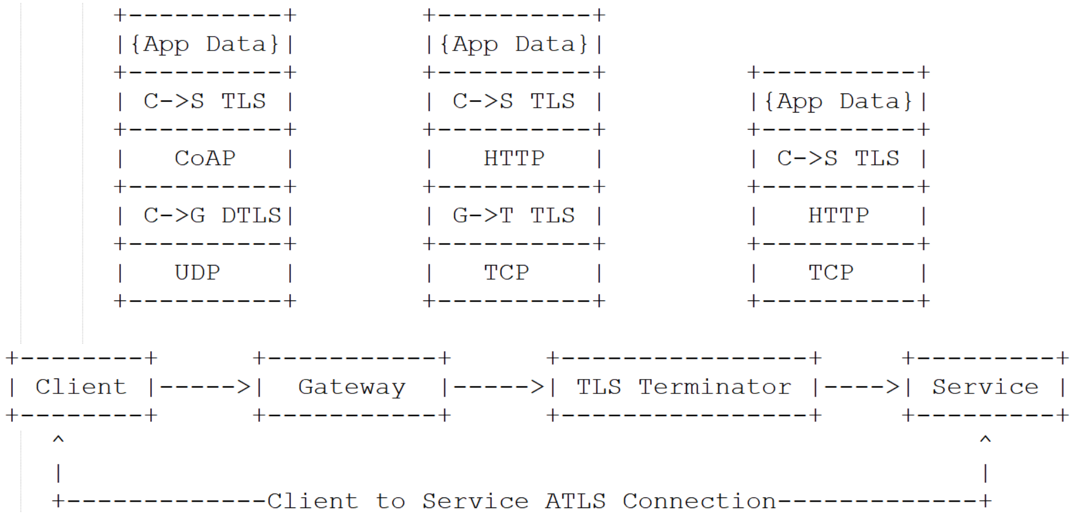


```
+---------------+
|               |
| Application   |
|               |
| +-------+     |              +---------+
| | App   |     |  Key Export  |         |
| | Data  |<----|<-------------|         |
| | Crypto|     |              |   App   |
| +-------+     |     TLS      |   TLS   |      +---------+
|    ^          |  Handshake   | Session |----->|   TLS   |
|    |          |   Records    |         |      |  Stack  |
|    |     +--->|<------------>|         |      +---------+
|    |     |    |              +---------+           ^
|    |     |    |                                    |?
|    |     |    |  Transport +-----------+   +------------+
|    |     |    |   Payload  | Transport |   | Transport  |
|    +-----+--->|<---------->|   Stack   |--->| Encryption |-->Packets
+---------------+            +-----------+   +------------+
```

Figure 6: TLS stack used for key agreement and exporting

Encrypted Data Transport Layering

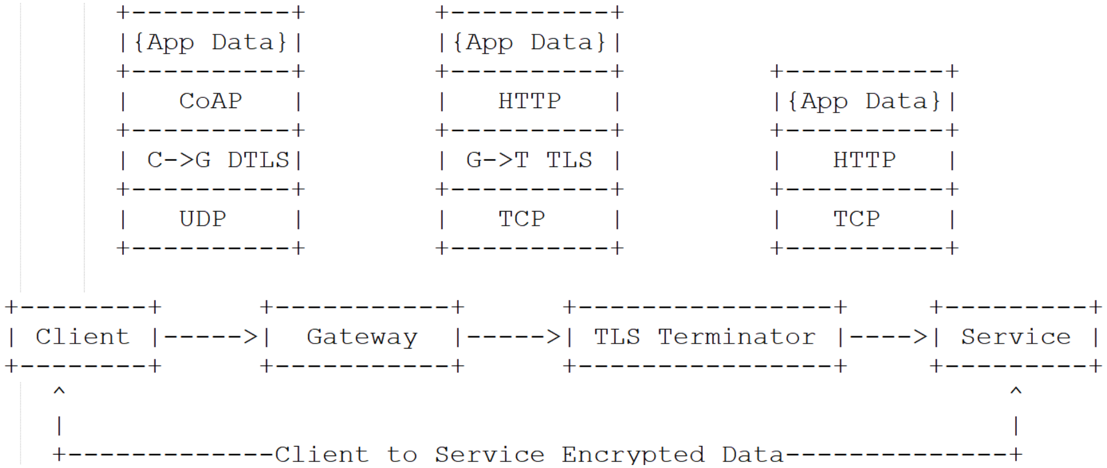
1. D/TLS Data Records



```
        +-----------+      +-----------+
        |{App Data} |      |{App Data} |
        +-----------+      +-----------+      +-----------+
        | C->S TLS  |      | C->S TLS  |      |{App Data} |
        +-----------+      +-----------+      +-----------+
        |   CoAP    |      |   HTTP    |      | C->S TLS  |
        +-----------+      +-----------+      +-----------+
        | C->G DTLS |      | G->T TLS  |      |   HTTP    |
        +-----------+      +-----------+      +-----------+
        |   UDP     |      |   TCP     |      |   TCP     |
        +-----------+      +-----------+      +-----------+

+---------+      +------------+      +-----------------+      +----------+
| Client  |----->|  Gateway   |----->| TLS Terminator  |---->| Service  |
+---------+      +------------+      +-----------------+      +----------+
  ^                                                               ^
  |                                                               |
  +-------------Client to Service ATLS Connection-------------+
```

2. Key exporting



```
        +-----------+      +-----------+
        |{App Data} |      |{App Data} |
        +-----------+      +-----------+      +-----------+
        |   CoAP    |      |   HTTP    |      |{App Data} |
        +-----------+      +-----------+      +-----------+
        | C->G DTLS |      | G->T TLS  |      |   HTTP    |
        +-----------+      +-----------+      +-----------+
        |   UDP     |      |   TCP     |      |   TCP     |
        +-----------+      +-----------+      +-----------+

+---------+      +------------+      +-----------------+      +----------+
| Client  |----->|  Gateway   |----->| TLS Terminator  |---->| Service  |
+---------+      +------------+      +-----------------+      +----------+
  ^                                                               ^
  |                                                               |
  +-------------Client to Service Encrypted Data--------------+
```