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

![Diagram of Bootstrapping Devices]

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

![Diagram 1: IoT Closed Network Gateway](image)

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

![Diagram 2: IoT Internet Gateway](image)
Implementation Options

1. D/TLS Data Records
   • Encrypted Data transported inside D/TLS Records

2. Key exporting
   • ATLS only used for handshake (2xRTT) and key exporting
   • Data encrypted by application using shared keys
Encrypted Data Transport Layering

1. D/TLS Data Records

2. Key exporting