PANA over TLS
(draft-ohba-pana-potls-01.txt)

Yoshihiro Ohba (yohba@tari.toshiba.com)
Shinichi Baba (sbaba@tari.toshiba.com)
Subir Das (subir@research.telcordia.com)

Objectives

- Specify a protocol for carrying authentication parameters over IP layer as per WG requirements
- Help the WG discuss outstanding issues such as PAA discovery, re-authentication, security threats

Design Policy

- Start from providing maximal level of security, however,
  - If it turns out that some of the security features are not needed for specific environments, the features can be removed or keep it as optional
    - Example: DI protection is one feature that is under discussion

Basic Features

- Authentication parameters including EAP PDUs are carried over TLS
  - Message integrity, encryption, replay protection and fragmentation is provided by TLS
  - Some EAP methods have their own protection mechanisms, but not all methods protect EAP Success/Failure
- TLS runs over reliable transport
  - Reliability and congestion control is provided by reliable transport
  - UDP has some advantage (e.g., bulk data transfer), but may not be suitable for TLS transport in terms of security
    - For example, an attacker can “randomly” insert integrity-broken TLS message to shutdown TLS connection due to invalid MIC

Message Format

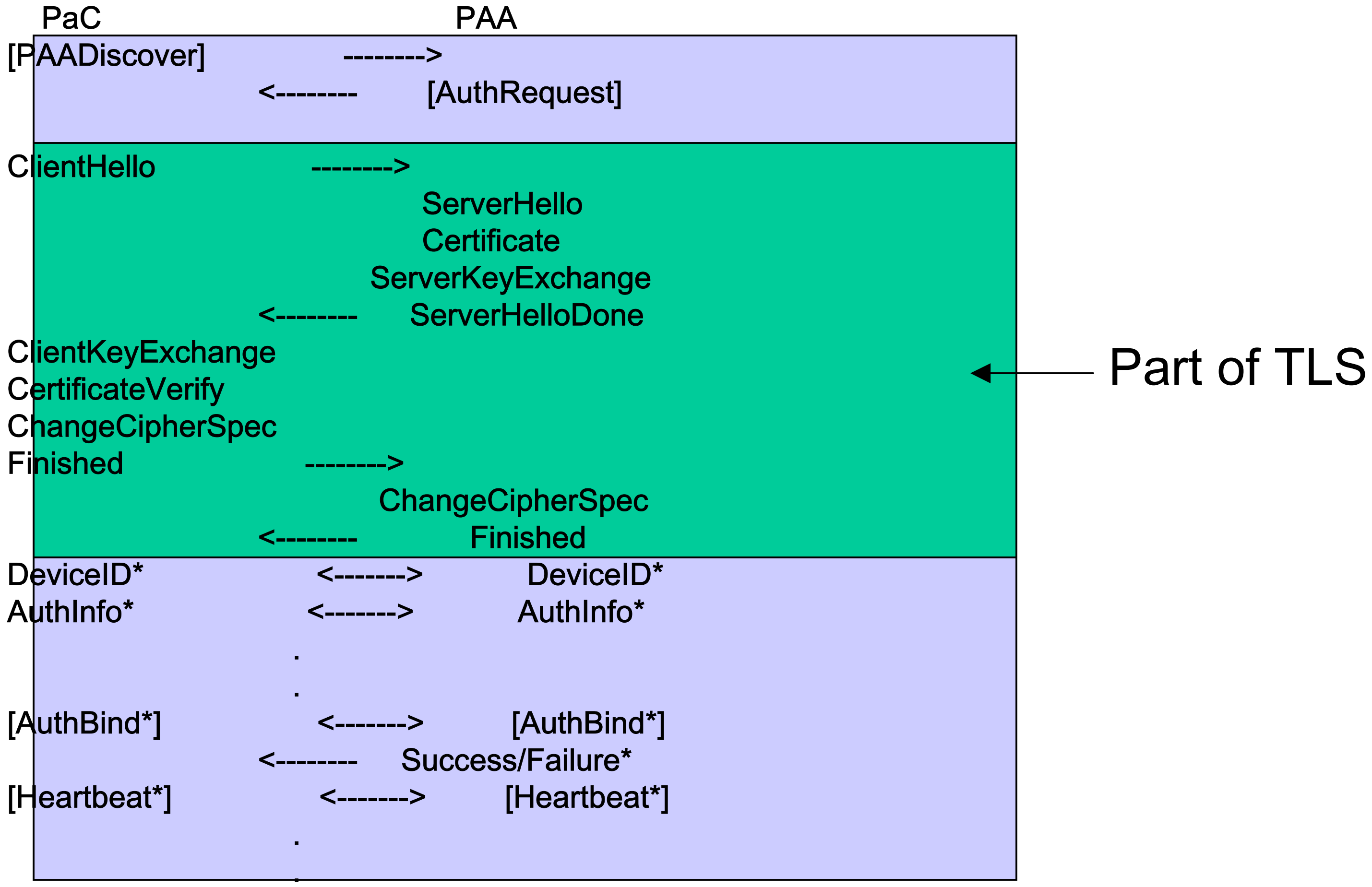
- Based on TLV (Type-Length-Value), with additional Subtype field

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type      |   Subtype    |           Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Payload
+----------------------------------------------------------
```

Authentication Modes and Types

- Authentication modes
  - Full Authentication
    - A new TLS master key is established
    - **AuthInfo** message is used for carrying EAP
  - Fast Authentication
    - Based on TLS session resumption
- Authentication types (defined in Full Auth. only)
  - One-way TLS authentication
    - TLS client certificate is **not** used
  - Mutual TLS authentication
    - TLS client certificate is used

Full Authentication Example (One-way TLS Authentication)



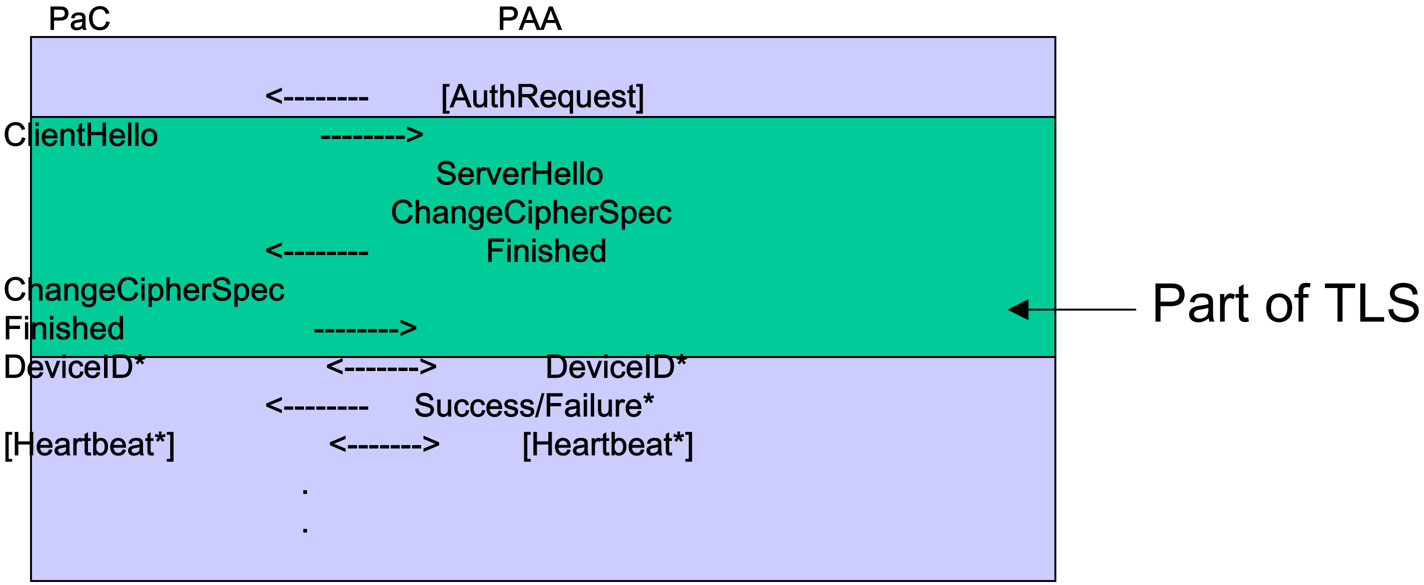
```
PaC                               PAA
[PAADiscover]          -------->
                 <--------      [AuthRequest]

ClientHello          -------->
                                ServerHello
                                Certificate
                            ServerKeyExchange
                 <--------     ServerHelloDone
ClientKeyExchange
CertificateVerify
ChangeCipherSpec
Finished             -------->
                             ChangeCipherSpec
                 <--------          Finished
DeviceID*             <------->        DeviceID*
AuthInfo*             <------->        AuthInfo*
                    .
                    .
[AuthBind*]           <------->       [AuthBind*]
                 <--------     Success/Failure*
[Heartbeat*]          <------->       [Heartbeat*]
                    .
                    .
```

Part of TLS

]

Fast Authentication Example



```
PaC                                 PAA

                  <---------      [AuthRequest]
ClientHello              --------->
                                ServerHello
                             ChangeCipherSpec
                  <---------        Finished
ChangeCipherSpec
Finished                 --------->
DeviceID*                 <------->         DeviceID*
                  <---------    Success/Failure*
[Heartbeat*]              <------->       [Heartbeat*]
                      .
                      .
```

Part of TLS

Authentication of Client

- No new security protocols or mechanisms
  - PoTLS uses TLS to carry any kind of existing authentication protocol including EAP
  - Any client identifier supported by TLS or EAP can be used
- Both PaC and PAA can authenticate each other
  - At least by using Mutual TLS Authentication
  - Or by using an EAP mechanism that supports mutual authentication
- IP address is required for PaC to run PoTLS

Authentication of Client (Cont’d)

- Capable of both periodic and on-demand re-auth.
  - By using Fast Authentication
  - Faster re-authentication is also possible (see slide 16)
- Both PaC and PAA can initiate initial auth. and re-auth.
  - Full and Fast Auth. can be initiated by both entities
- DI is carried explicitly in PANA payload and protected with TLS

Authorization, Accounting and Access Control

- Provides binary authorization (Success/Failure)
  - Success message contains a subtype for indicating whether transport connection should stay opened (for re-authentication purpose)
- Access control
  - Mapping between PaC identity and DI is maintained in PAA
  - Access control is assumed to be done outside of PoTLS
- Accounting data
  - Carrying accounting data is out of the scope of PoTLS

Authentication Backend

- Backend AAA protocol is not mandatory for PoTLS to work
  - It can be used if required

Disconnect Indication

- Implicit and explicit disconnect indications are supported
  - Implicit indication: based on re-authentication
    - If re-authentication fails within a specific time period, peer is considered as disconnected
  - Explicit indication is based on explicit TLS connection termination sequence
    - Performed when a PaC or PAA wants to disconnect
- Both types of disconnect indications can be initiated from both PaC and PAA

Location of PAA

- PAA is assumed to be on the same link as PaC
- No assumption for co-location of PAA and EP
- Four methods are defined for PAA Discovery mechanism
  - Manual configuration, DHCP, multicast query and notification from PAA
  - Details are for further study

Secure Channel

- Assumption: an attacker can read or modify the information exchanged between PaC and PAA
- TLS is used for protecting authentication message exchange
  - Some EAP methods also have protection mechanisms
  - Our assumption is that not all EAP methods are secure enough

Performance

- Utilizing TLS session resumption functionality for quick re-authentication
- Optional Authenticated Heartbeat Protocol* is defined for further improvement
  - A short request/response message is exchanged over TLS
  - Used for implicit disconnection detection

*the name is subject to change

Reliability, Congestion Control and Misc.

- PoTLS uses over reliable transport
  - Reliability and congestion control is provided by transport layer
  - Re-transmission in EAP is turned off, except for the messages that require a response based on user input
- PoTLS works for both IPv4 and IPv6
- Weakness for blind masquerade attack is no worse than that for TCP SYN attack
  - PAA does not do any cryptographic computation before 3(4)-way handshake completes at transport layer

A New Issue: Cryptographic Bindings

- If multiple auth. methods in a single auth. conversation are not cryptographically bound, MiTM attacks is possible
  - Under discussion in the EAP WG
- PoTLS provides cryptographic binding between TLS session and phase2 key created as a result of authentication message exchange, e.g., EAP
  - by exchanging AuthBind message that contains a PRF value calculated from Phase2 key
  - AuthBind message is carried over TLS

Open Question

- Question: Should the WG assume that EAP is secure enough?
- Why: Since we believe that PANA protocol design will heavily depend on EAP
  - Not all EAP methods have strong protection mechanism

Thank you!