Secure Network Access Authentication (SeNAA)

draft-forsberg-pana-secure-network-access-auth-01.txt

Dan Forsberg *(dan.forsberg@nokia.com)*

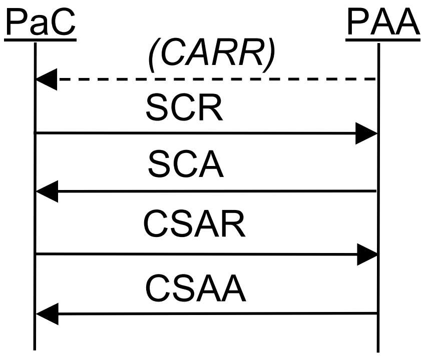
Jarno Rajahalme *(jarno.rajahalme@nokia.com)*

Nokia Research Center

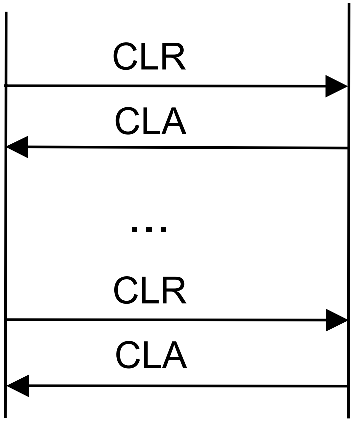
Discussion Points

- Quick Overview of SeNAA
- SeNAA protocol design:
  - Why UDP?
  - Why TLS?
  - Why Diameter Message Formatting?
  - Why SeNAA?
- Requirements Mapping
- Security Threats Mapping
- Open Issues in the Current Draft (01)
- Issues to be considered?

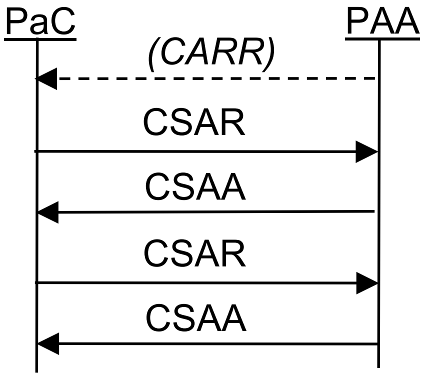
Quick Overview of SeNAA



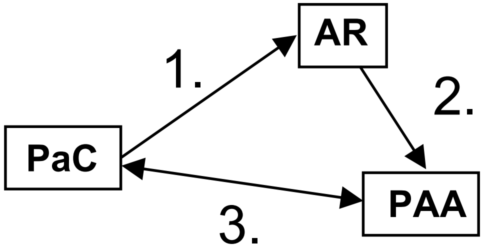
Optional Phase 1: Initial Network Authentication with TLS from PaC (*from PAA*)



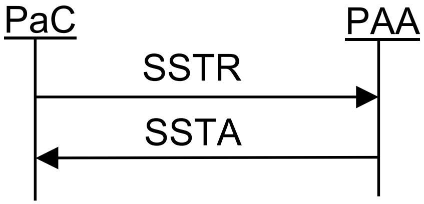
Phase 2: User Authentication with EAP



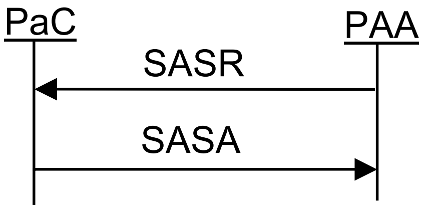
Re-Authentication with TLS from PaC (*from PAA*)



PAA Discovery



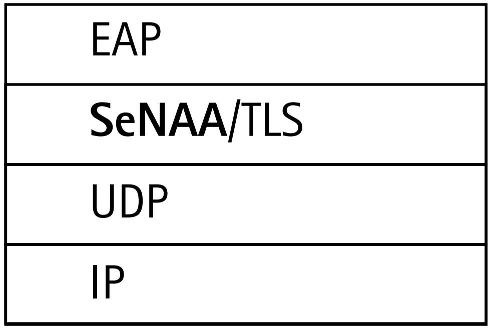
Session Termination from PaC



Session Termination from PAA

Why UDP?

- Lightweight and IP version independent
- Supports user level applications with port numbers
- Connectionless: better support for mobility



EAP

SeNAA/TLS

UDP

IP

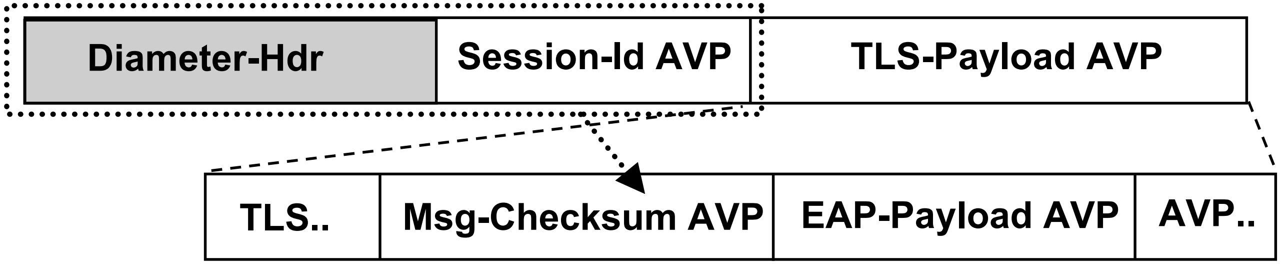
Protocol Stack

Why TLS?

- Provides integrity protection, replay protection, message authentication, data compression and privacy (MitM!)
- Local Security Association (LSA) for re-authentication and session resumption
- Provides key material for per-packet authentication (IPSec)
- Network authentication and possibility for client authentication
- Widely used and IP address (and version) independent
- Supports multiple connections inside one session(?)

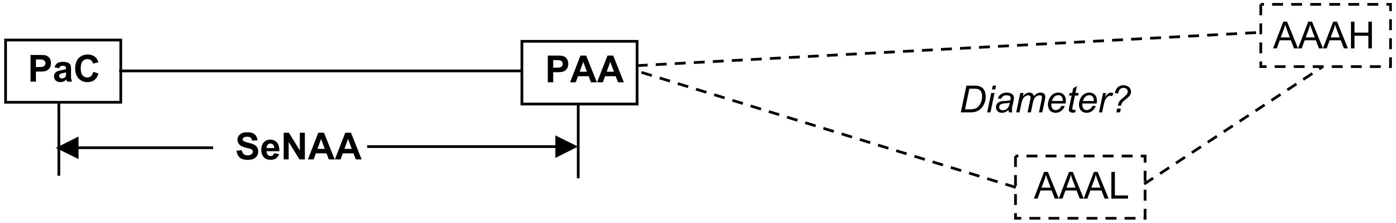
Why Diameter Message Formatting?

- Existing, well defined and extendible message formatting in the same area (AAA).
- Diameter header provides material for duplicate packet detection (End-to-End Id) and request/response mapping (Hop-by-Hop Id).
- Facilitates interworking with backend AAA protocol (same code for handling the messages).
- Easy to add new AVPs and command codes.
- Result-Code AVP supports error reporting.



Why SeNAA?

- Simple Request – Response style protocol.
- By default two phases: Phase 1 - network authentication (TLS) and Phase 2 - user authentication (EAP).
- Request re-transmissions and Diameter header info together provide reliable transport for TLS.
- Phase 1 is optional: SeNAA is independent from TLS.
- EAP method independent (MitM!).
- Need to carry information that is not included in the EAP (DI etc.).



Requirements Mapping (1/3)

- Req. 4.1.1 Authentication of Client
  - SeNAA uses User-Name and DI. User-Name is used in the beginning for AAA message routing and access network certificate selection.
  - SeNAA carries EAP.
  - TLS session provides key material for example for IPSec
  - TLS is used for network authentication (possibly for client authentication)
  - Current SeNAA draft is not clear about PAA initiating the authentication. A new message called Client-Authentication-Request-Request (CARR) is to be defined. PAA sends CARR when it requires authentication from PaC.
  - SeNAA protects the PaC DI with TLS. PAA DI is not protected in the current draft. SeNAA probably should do that.
- Req. 4.1.2. Authorization, Accounting and Access Control
  - Binary authorization result with Result-Code AVP
  - Accounting data is not carried by SeNAA.

Requirements Mapping (2/3)

- Req. 4.1.3. Authentication Backend
  - Independence of backend authentication protocol.
- Req. 4.1.4. Identifiers
  - SeNAA supports multiple DIs (L2 address + IPv6 address for example). New types can be defined, when needed. Currently none specified.
  - DI is carried from PaC to PAA, which binds it to the authenticated session.
- Req. 4.1.5. IP Address Assignment
  - Assumes IP connectivity to PAA and AR
- Req. 4.2.2. Disconnect Indication
  - TLS is used for LSA. Local timer for LSA?
  - SeNAA provides explicit disconnect indication (SSTR & SASR).
- Req. 4.2.3. Location of PAA
  - PAA at the same link is ok
  - SeNAA's PAA discovery happens through the advertising router, which forwards the message to PAA. PAA answers directly for PaC.
  - SeNAA does not specify any protocol for PAA ←→ EP communication. SeNAA approach assumes that PAA and EP are co-located.

Requirements Mapping (3/3)

- Req. 4.2.4. Secure channel
  - TLS provides secure channel.
- Req. 4.3.
  - UDP as a carrier. The sessionless nature of UDP suits well for mobile environments.
- Req. 4.4. Performance
  - TLS as LSA
  - UDP as a carrier
- Req. 4.5. Reliability and Congestion Control
  - SeNAA provides re-transmission and duplicate packet check. TLS provides integrity.
- Req. 4.6.1. IP version independent
  - OK
- Req. 4.6.2. DoS attacks
  - Depends on TLS. Needs more analysis.

Threat Requirements Mapping (1/2)

- Req. 1 PANA MUST not assume that the discovery process is protected.
  - Network access authentication through TLS server certificate. PAA DI protection also needed to prevent DoS attack (PAA IP address not available).
- Req. 2. PANA SHOULD protect the identity of the PaC from eavesdropping and polling attack.
  - DI is protected with TLS.
  - User-Name AVP contains dummy user part or encrypted user part. Not specified in the draft.
- Req. 3. MitM attack
  - Mutual authentication with TLS or with EAP method and TLS.
  - SeNAA requirement is that plain password based EAP methods MUST not use same credentials with SeNAA as compared to the signaling without SeNAA → SeNAA doesn't specify how EAP session and TLS session secrets are bound together.
- Req. 4. PANA MUST be resistant to replay attacks.
  - TLS is resistant to replay attacks.

Threat Requirements Mapping (2/2)

- Req. 5. Disconnect and revocation messages MUST be authenticated
  - SeNAA explicit disconnect requests (SSTR & SASR) and answers (SSTA & SASA) messages are protected.
- Req. 6. & 7. Key derivation
  - TLS master secret can be used to derive keys for per-packet authentication
- Req. 8. PANA per-packet authentication MUST provide anti-replay service
  - TLS protects against replay attacks.
- Req. 9. PANA should not assume that the client has a valid IP address.
  - Relates to per-packet authentication..

Open Issues in the Current Draft (-01)

- PAA initiating: Client-Authentication-Request-Request (CARR) is not defined in the draft.
    - EPs/ARs can send this also.
    - Includes PAA’s address.
- User-Name AVP and EAP-Identity.
- What kind of signaling without TLS.
- MAC versus checksum.
- PAA’s DI protection, MitM, DoS attacks.
- IDEA: SeNAA messages could easily be mapped to DHCPv6 messages.