# Channel Binding Support for EAP Methods

Charles Clancy, Katrin Hoeper

<draft-clancy-emu-aaapay-00>

<draft-clancy-emu-chbind-00>

# Definition

- *EAP channel bindings (c.b.)* (as defined in the drafts) provide a consistency check of information advertized to peer and known by the authentication server from an authenticator acting as a pass-through device during an EAP session.

# Goals

- Bind information advertized by an authenticator to the channel and verify its consistency to prevent attacks by rogue authenticators.
  - E.g. prevent “lying NAS attacks”

# Proposed Method

Phase 1. Information exchange

- Peer sends $info_1$ to server
- [Server sends $info_2$ to peer]

Phase 2. Consistency check

- Server verifies consistency and sends *result* to peer
- [Peer verifies consistency and fails if inconsistent]

# Data Exchange

- I-D.clancy-emu-aaapay
  - Defines way to encapsulate arbitrary Diameter AVPs in the protected channels of existing EAP methods
  - Includes GPSK, PSK, PAX, TTLS, FAST
- Channel binding information encoded in Diameter AVPs (or RADIUS TLVs using backward compatibility)
- Data exchanged as part of EAP messages in end-to-end integrity-protected channel

# Design Choices

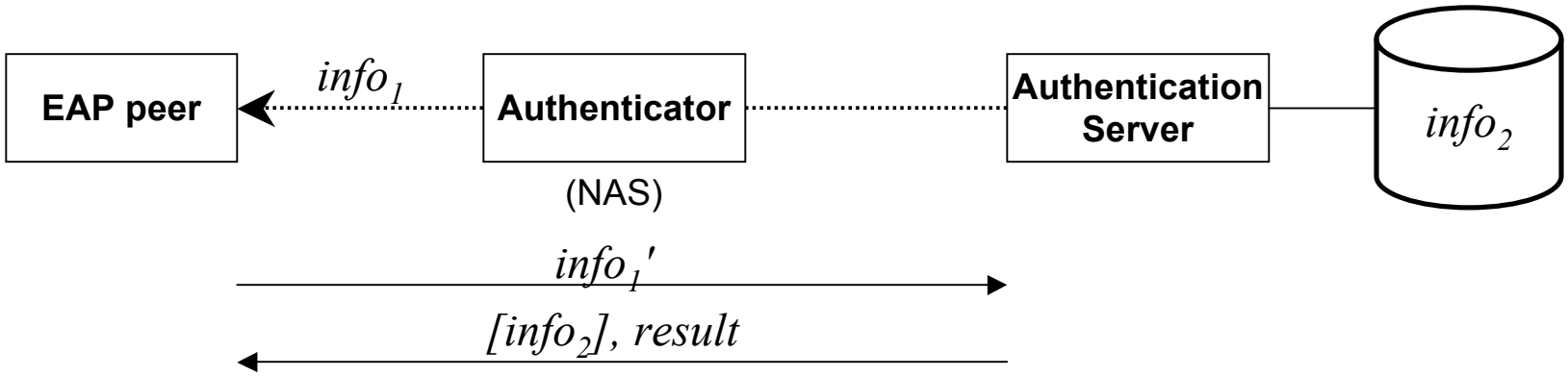
- Server performs consistency check
- Explicit data exchange and verification
  - As opposed to implicit, e.g. by hashing identity and other information directly into keys
- Benefits:
  1. *Enterprise:* server more likely to be capable of recognizing whether different addresses belong to same device
  2. *Service Provider:* more likely to know details of contractual roaming agreements
  3. Easy add-on solution for EAP methods: no modifying EAP key derivations, message flow or state machine nor adding new algorithms or messages
  4. Allows for fuzzy comparisons

# Binding Information

- Exact parameters to bind are open to discussion
- Document provides placeholders for some EAP lower layers
  - IEEE 802.11
    - SSID, BSSID, RSN IE (if present)
  - IKEv2, IEEE 802.16 and other EAP lower layers
    - TBD

# Our Trust Model

- Honest peer & authentication server; may be dishonest authenticator




- Trust relationships
  1. server trusts that $info_1 = info_1'$
  2. peer trusts *result*
  3. server trusts stored $info_2$

# EAP Method Requirements

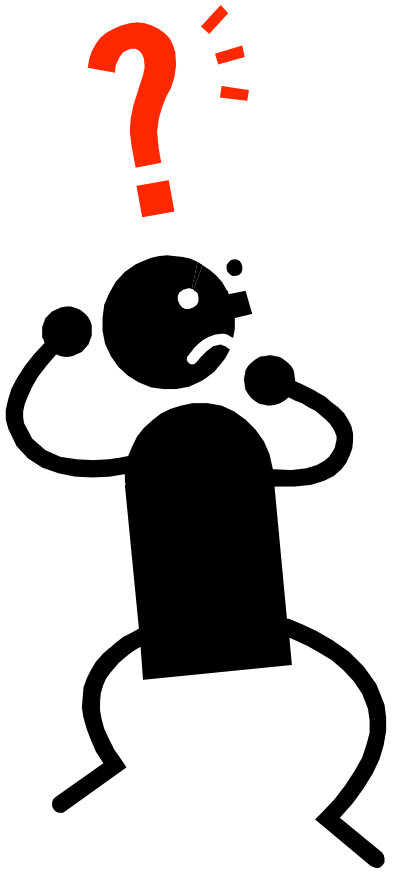
- Peer ↔ AS trust relationship can be established by any EAP method with the following properties:
  - mutual authentication between peer and server
  - derivation of keying material including an integrity key
  - $info_1$ sent from peer to server over end-to-end integrity-protected channel
  - *result* (and optionally $info_2$) sent from server to peer over end-to-end integrity-protected channel

# System Assumptions

- Assume server maintains protected database of $info_2$
- Consistency check requires server to be capable of comparing provided information
  - *Enterprise:* validate information on a per-authenticator basis
  - *Service Provider:* validate information on a per-network basis
- Both must be ensured outside EAP

# Future Work

- It's a start, but much works remains to be done:
  - message flow, incl. EAP-success/failure cases
  - example attacks
  - binding information
  - security considerations
  - …



Questions?

Comments?