HOKEY WG
Interim Meeting

23 January 2007
Cisco, San Jose, CA

Chairs: Charles Clancy, Glen Zorn

Administrivia

- Note Takers
- Attendance Sheets
- Disclaimer:
  - INTERIM meeting
  - No final decisions can be made
  - Conclusions must be discussed on the mailing list
- Goal:
  - Figure out approach to re-auth before Prague

Agenda (Part 1: PS/Hierarchy)

- 9am – 9:20: Introduction
  - Introduction (5 min)
  - Note Takers (5 min)
  - Attendance (5 min)
  - Agenda Bashing (5 min)
- 9:20 – 9:50: Problem Statement Draft

  `draft-ietf-hokey-reauth-ps-00`
- 9:50 – 10:00: EMSK Keying Hierarchy

  `draft-ietf-hokey-emsk-hierarchy-00`
- 10:00 – 10:30: Discussion

Agenda (Part 2: Protocol Drafts)

- 10:30 – 10:50: EAP ER

  draft-vidya-eap-er

- 10:50 – 11:10: EAP EXT

  draft-ohba-hokey-emu-eap-ext

- 11:10 – 11:30: Keying Hierarchy for Managing Wireless Handover Security

  draft-nakhjiri-hokey-hierarchy

- 11:30 – 12:15: Lunch

Agenda (Part 3: Major Design Issues)

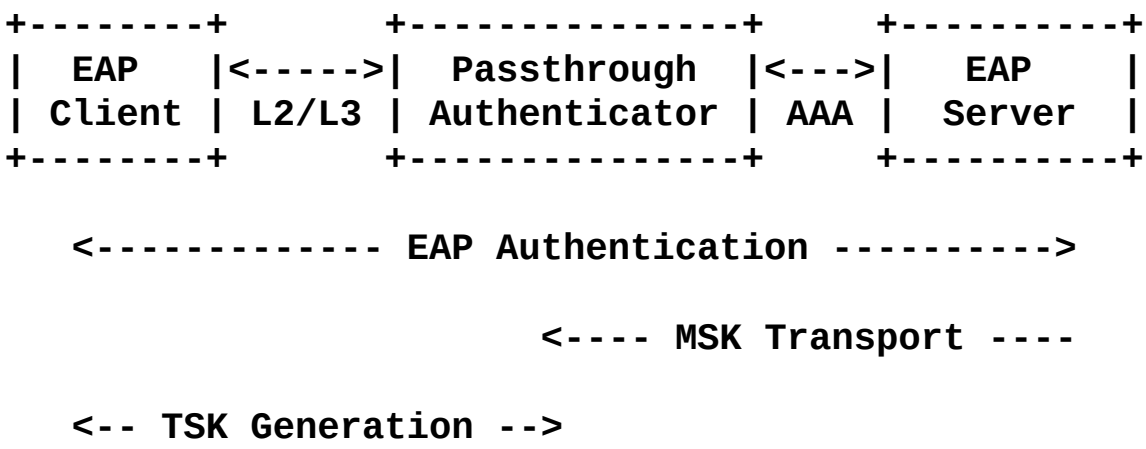
- 12:15 – 5pm: Protocol Design Issues
  - Goal: form consensus on how reauth protocol should operate
  - Key discussion points:
    - Keying (hierarchy vs keywrap, MSK vs EMSK)
    - Protocol transport (code-based, type-based, or other)
    - Backwards compatability (L2 signaling, timeouts, etc)
    - Affect on lower layers (state machine, etc)
    - Peer vs server initiated

Reauth Problem Statement

- WG Document (16 January 2007):
  - draft-clancy-hokey-reauth-ps → draft-ietf-hokey-reauth-ps
- Fusion of:
  - draft-vidya-eap-reauth-ps
  - draft-nakhjiri-aaa-hokey-ps

Reauth PS Overview

- No new terminology – use RFC 3748 / EAP keying draft terminology



- Dealing with one logical authenticator (may be multiple physical devices)

Reauth Problem Statement

- No method-independent way to do EAP re-authentication
- Need such a way for fast re-authentication and handoff between authenticators
- Roaming
  - mention, but don't directly address
  - re-auth solution MUST NOT prevent fast roaming in the future

Reauth Design Goals (1/2)

- Lower Latency Operation
  - fewer RTs than full reauth
  - no absolute RT or timing requirements
- EAP Lower-Layer Independence
  - MAY require support from lower layer
  - MUST accommodate inter-technology handoff
- EAP Method Independence
  - No changes to current EAP methods
  - No restrictions on future EAP methods

Reauth Design Goals (2/2)

- AAA Protocol Compatibility
  - MUST be compatible with RADIUS and Diameter
  - MAY require extensions
  - MUST satisfy draft-housley-aaa-key-mgmt
- Compatibility
  - SHOULD coexist with existing EAP implementations
  - SHOULD be compatible with other fast-handoff techniques
  - MUST not interfere with CAPWAP and 11r

Security Goals (1/2)

- Key context and domino effect
  - Keys MUST have name, scope, context, lifetime
  - MAY require key scope exchange
  - key2=f(key1) →
    - lifetime(key2) ≤ lifetime(key1)
    - compromise(key2) ≠ compromise(key1)
- Key freshness
  - cryptographic key separation
  - need ability to refresh keys (and child keys?)

Security Goals (2/2)

- Authentication
- Authorization
- Channel Binding
  - Intermediate Entities
  - EAP Peer, Authenticator, Server
  - AAA Proxies?
- Transport Aspects

Use Cases

- IEEE 802.11r
  - Key root (PMK-R0) moved away from the network edge, better physical security
- CAPWAP
  - Secure handoff between ACs
- Other
  - Handoff between technologies
- Out of scope:
  - Handoff between home/visited AAA servers (roaming)

Conclusion

- Consensus on everything?

EMSK Hierarchy

- Minor edits to draft-salowey-eap-emsk-deriv
- Became draft-ietf-hokey-emsk-hierarchy

- Consensus?