PS: EAP re-authentication and key management

draft-vidya-eap-reauth-ps
Lakshminath Dondeti, ldondeti@qualcomm.com
Vidya Narayanan, vidyan@qualcomm.com
IETF-67, San Diego, CA, November 2006
Contents

• EAP re-authentication, defined

• Re-authentication problem statement

• Design goals and constraints in solving the problem

• Necessary Extensions to EAP keying hierarchy to solve the problem

• Use cases and applicability

• Conclusion and Next steps
EAP re-authentication, defined

• EAP keying I-D defines it as:
  – EAP authentication between an EAP peer and a server with whom the EAP peer shares valid unexpired keying material.

• RFC 4187 defines, fast re-authentication as:
  – authentication exchange that is based on keys derived upon a preceding full authentication exchange.

• 4187’s definition is closer to what we want:
  – We want “efficient” re-authentication
  – Avoid having to do a full method run with home
  – Also need to be method agnostic
EAP Re-authentication, as per today’s standards

Peer (UE)  Auth1  Auth2  AAA-L  AAA-H

EAP Req/Identity  EAP Resp/Identity  Initial EAP Exchange  EAP Success (MSK1)

Full EAP Method Exchange

MSK1, EMSK1  EAP Success  MSK1, EMSK1
EAP Re-authentication, as per today’s standards

Peer (UE) | Auth1 | Auth2 | AAA-L | AAA-H
---|---|---|---|---

**Initial EAP Exchange**
- **EAP Reg/Identity**
- **EAP Resp/Identity**
- **Full EAP Method Exchange**
- **EAP Success**
- **MSK1, EMSK1**
- **EAP Success (MSK1)**

**Subsequent EAP Exchanges**
- **EAP Reg/Identity**
- **EAP Resp/Identity**
- **Full EAP Method Exchange (or, Method-Specific Fast Re-authentication)**
- **EAP Success**
- **MSK2, EMSK2**
- **EAP Success (MSK2)**
- **MSK2, EMSK2**
Motivation (1/2)

• A full method run upon each time a peer moves to an authenticator
  – Is Expensive
  – Introduces unacceptable amt of latency

• Some methods have means to reduce computational complexity; that’s not enough
  – Need a method-independent solution
  – Need a solution that reduces latency and computational complexity
Motivation (2/2)

• The other problem is interaction with the home network
  – Even if roundtrips are reduced, trips to home take too long
  – 3GPP AKA allows a visited domain server to download AKA vectors to speed-up re-authentication
  – Need something similar
    • But also a solution that is method independent
Design goals and constraints

• Low latency operation

• EAP lower layer independence

• Inter-technology handover

• EAP method independence

• AAA protocol compatibility

• Compliance to Housley Criteria
Root key selection

• MSK is delivered to the authenticator

• MSK is used differently by different lower layers and protocols
  – IKEv2 uses it for entity authentication
  – 802 lower layers use it for TSK generation
    • 802.11i uses the first 16B and 11r uses the rest
    • 802.16e uses 26B of the MSK (Verify this)

• Conclusion: use the EMSK hierarchy
  – For lower-layer independence
  – To avoid changing MSK delivery and usage semantics
Keying considerations for Re-authentication

• Need a key to support Re-authentication
  – A key to provide proof-of-possession
  – A key to derived keys to serve as an MSK does at a new authenticator

• Need key hierarchy extensions to support visited domain operation.
Applicability and use cases (1/2)

• 802.11r provides a solution to avoid EAP re-authentication
  – There are some gaps in the solution
    • Key transfer between key holders is not defined
    • Limited to mobility within an ESS
  – We may provide an alternative solution and/or complementary solution
Applicability and use cases (2/2)

- CAPWAP provides a solution for a peer moving between WTPs of an AC
  - What happens when a peer moves beyond the WTP’s coverage area?
- Inter-technology roaming
  - Re-authentication when a peer moves from a WLAN AP to a 802.16 BS
- Inter-domain roaming
  - Re-authentication when a peer moves from one administrative domain to another
Summary and next steps

• EAP re-authentication and associated key hierarchy requirements explained

• draft-vidya-eap-reauth-ps-00 contains a detailed description of all aspects covered in this presentation
  – Propose to make it a WG document
  – Invite others to work with us on it