Extensions to EAP Keying hierarchy for Efficient Re-authentication and Visited domain Keying

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

• EAP keying hierarchy
• Motivation for extending the key hierarchy
• Requirements on extending the key hierarchy
  – Driving applications
• Proposed extensions
• Summary and next steps
EAP keying hierarchy: 802.11i, r

Long Term Credential

MSK

EMSK

PMK-R0

PMK-R1, ... PMK-R1

TSK1, ... TSKn

PMK

TSK

Figure shows the existing 802.11r key hierarchy

This key hierarchy does not use the EMSK; the second half of the MSK is used to derive the R0-Key

This is not a universal model used by other architectures employing EAP.
Low Latency Re-authentication Requirements

- It is unacceptable to have to go back to the home domain upon every handoff in a visited domain
  - Access to AAAH may be through one or more AAA proxies

- A single roundtrip protocol that can result in fresh keying material for new points of attachment is desirable
  - The protocol must be executable with the visited domain
  - The resulting key material should be as strong as in the first full authentication case

- The protocol must be EAP method independent
  - Makes executing with the visited domain possible
    - Method specific operation limited to nodes and their home domain

- Ideally, the protocol should be executable in parallel with connection establishment
  - Security becomes undesirable when any latency or overhead is added to the critical path 😊
EAP Extensions – Constraints

• We don’t quite have a free hand in designing EAP extensions
  – To some extent, we must design around the current designs and usage models of EAP

• MSK cannot be used for new keying material
  – Usage of MSK disparate over different lower layers

• EAP authenticators and visited domain entities must not be required to support EAP methods

• The key delivery semantics from re-authentication must be similar to MSK delivery
  – Lower layers must be able to use the key for the same purpose as the MSK (e.g., for TSK derivation)
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 40B or 20B of the MSK
- Conclusion: use the EMSK hierarchy
  - For lower-layer independence
  - To avoid changing MSK delivery and usage semantics
Solution requirements

• Method-independent protocol for efficient re-authentication
  – Access agnostic; can be used for inter-technology handoffs
  – Proof of possession of key material of an earlier authentication
  – Visited-domain EAP-ER capability
  – Preferably a single roundtrip re-authentication protocol

• Key Generation in EAP-ER
  – EMSK-based hierarchy defined for this purpose
    • MSK cannot be used for this in an access-agnostic manner
  – Re-authentication MSKs (rMSK)
    • Serves the same purpose as an MSK
  – Visited Domain Keying hierarchy
    • V-rMSKs derived from this hierarchy for re-authentication in a visited domain
Requirements on EAP keying hierarchy

• Need a root-key or USRK for EAP-ER
  – re-authentication Root Key (rRK, derived from EMSK)

• A key to prove being a party to the full EAP method-based authentication
  – This is used in a proof of possession exchange between the peer and the server
    • A re-authentication Integrity Key (rIK, derived from the rRK)

• A new MSK specific to each authenticator that the peer associates with
  – A re-authentication MSK (rMSK1, rMSK2, …)
  – Derived from the rRK
Re-auth key hierarchy for home domain
Key derivation

- $rRK = \text{prf}^+(K, S)$, where,
  - $K = \text{EMSK}$ and
  - $S = rRK \text{ Label}$
    - (“EAP Re-authentication Root Key”)

- $rRK_{\text{name}} = \text{NDF-64}(\text{EAP Session-ID, } rRK \text{ Label})$

- $rIK = \text{prf}^+(rRK, \text{"Re-authentication Integrity Key"})$

- $rIK_{\text{name}} = \text{prf-64}(rRK, \text{"rIK Name"})$
Visited domain requirements on the EAP keying hierarchy

• Need a USRK, visited-domain root key (VRK) for visited domain keying purposes
  – This is to be maintained at the peer and the home EAP server

• Each visited-domain needs a root key to manage domain specific keying requirements
  – A Visited-domain Master Session Key (VMSK) per domain is derived and delivered by the home EAP server
    • Each VMSK is held by the visited-domain EAP server and the peer

• The rest of the key hierarchy is similar to EMSK hierarchy
  – A V-rRK maps to the rRK
  – V-rIK maps to the rIK
  – V-rMSKi maps to rMSKi
Visited Domain Re-authentication
Key Hierarchy

VMSK

V-rRK

V-rIK  V-rMSK₁  …  V-rMSKₘ

TSK₁  TSKₘ
Example Derivation of VMSK
VMSK Key derivation

• VRK = prf+ (K, S), where
  – K = EMSK and
  – S = “EAP Visited domain Root Key”

• VRK_name =
  NDF-64( EAP Session-ID, VRK Label )

• VMSK = prf+ (K, S), where
  – K = VRK and
  – S = Server ID || Domain Name

• VMSK_name =
  NDF-64( EAP Session-ID, Server ID || Domain Name )
Summary and Next steps

• Two extensions to the EAP keying hierarchy are proposed
  – Specified derivation of two USRKs
    • rRK for re-authentication
    • VRK for Visited-domain keying purposes
• From the rRK, a key to prove possession, one or more keys for new authenticators are derived
• From the VRK, visited domain MSKs are derived
• Specified in
  – draft-vidya-eap-er-01
  – draft-dondeti-eap-vkh-00
• The group is requested to adopt these as WG items