Pre-authentication
Problem Statement
(draft-ohba-preauth-ps-00.txt)

Yoshihiro Ohba
Ashutosh Dutta
Srinivas Sreemanthula
Alper Yegin
Bernard Aboba
Outline

- EAP Pre-authentication
- Pre-authentication scenarios
- Pre-authentication AAA requirements
- Scope issues
EAP pre-authentication

• Definition [draft-ietf-eap-keying-15]
  “The use of EAP to pre-establish EAP keying material on an authenticator prior to arrival of the peer at the access network managed by that authenticator”

• Example usage of EAP pre-authentication: IEEE 802.11i pre-authentication
  – Defined for intra-ESS transitions

• HOKEY WG aims to make EAP pre-authentication to
  – Work across multiple ESS’s
  – Work across multiple access technologies
Scenario 1: Direct Pre-authentication

- Generate MSK with the authenticator-2 by executing EAP through it.
Scenario 2: Indirect Pre-authentication

- Generate MSK with the authenticator-2 by executing EAP through it.
Indirect Pre-authentication Layering Model

Mobile Node

- EAP Peer
- MN-SA Signaling Layer

Serving Authenticator

- Pre-authentication Forwarding
- MN-SA Signaling Layer
- SA-TA Signaling Layer

Target Authenticator

- EAP Authenticator
- MN-SA Signaling Layer
Pre-authentication AAA Requirements

• AAA requirements related to EAP pre-authentication need to be identified (See draft-nakhjiri-preauth-aaa-req-00 for details)
  – Distinguishing normal authentication from pre-authentication
  – Pre-authentication life-time
  – Re-pre-authentication
  – Post handover procedure
  – Session resumption or key caching
  – Multiple pre-authentication
  – Provisioning of serving network information
  – Inter-media pre-authentication
  – Network-controlled pre-authentication

• AAA requirements may affect MN-TA, MN-SA and SA-TA signaling design
In-Scope Pre-authentication Scenarios

• EAP pre-authentication authenticator is expected to use the same layer and the same protocol as the original EAP authentication used for the authenticator

• Example: Direct pre-auth where PANA or EAPoL2 is used for both EAP auth/pre-auth
  \[(\text{EAP auth, EAP pre-auth}) = (\text{PANA, PANA}), (\text{802.11i, 802.11i})\]
Out-of-Scope Pre-authentication Scenarios

• Direct pre-auth where EAPoL2 is used for EAP auth but EAPoL3 is used for EAP pre-auth
  \[(EAP \text{ auth}, EAP \text{ pre-auth}) = (802.11i, \text{ PANA})\]

• Indirect pre-auth where EAPoL2 is used for MN-SA signaling
  \[(EAP \text{ auth}, EAP \text{ pre-auth}) = (802.11i, 802.16e)\]

• Architectural impacts need to be analyzed before expanding the scope
  – AD suggested to have a design team to work on this outside of the HOKEY WG
Possible HOKEY Scope on Pre-authentication Work

• In-scope Work: Defining EAP pre-authentication requirements and solutions that are applicable to any protocol

• Out-of-scope Work:
  – Defining EAP pre-authentication solutions specific to particular protocols, e.g., Diameter, RADIUS, PANA, 802.1X
  – Defining a solution for authenticator discovery
    • Work can be done outside of IETF (e.g., IEEE 802.21)
Recent comments by B. Aboba

- There is an missing assumption that the mobile does not want to maintain context for two media simultaneously, e.g., power management concerns
  - Otherwise, it is possible to perform normal EAP authentication over new interface while preserving the connectivity to the current interface
- Be very specific about which handover scenarios you are trying to solve
  - Scenarios where target authenticators are easily discovered would be easy to solve
Next Step

• Add statement on out-of-scope scenarios
• Reflect B. Aboba’s comments