Pre-authentication
Problem Statement
(draft-ohba-preauth-ps-01.txt)

Yoshihiro Ohba
Ashutosh Dutta
Srinivas Sreemanthula
Alper Yegin
Mahalingam Mani
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
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
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
  – Network-controlled pre-authentication

• AAA requirements may affect MN-TA, MN-SA and SA-TA signaling design
HOKEY Charter in pre-authentication

• “EAP re-authentication and EAP pre-authentication authenticator are expected to use the same layer and the same protocol as the original EAP authentication used for the authenticator.”

• Reason for this restriction: Inter-technology pre-authentication has technical issues that need to be studied
  – Authenticator discovery
  – Context binding
Pre-authentication issue 1: Authenticator discovery

• In general, pre-authentication requires an address of a target authenticator to be discovered either by a mobile node or by a serving authenticator prior to handover

• An authenticator discovery protocol is typically defined as a separated protocol from a pre-authentication protocol

• When a target authenticator uses link-layer EAP transport for both normal authentication and pre-authentication, target authenticator discovery is typically defined in each link-layer technology
  – E.g., 802.11k and 802.16e

• For other cases, a mechanism for discovering an IP address of target authenticator is needed
  – (IP address, link-layer address) mapping needs to be resolved
Pre-authentication issue 2: Context binding

- A mechanism is needed to bind link-layer independent context carried over pre-authentication signaling to the link-layer specific context of the link to be established between the mobile node and the target authenticator
  - **Link-layer independent context**: the identities of peer and authenticator as well as MSK
  - **Link-layer specific context**: link-layer addresses of peer and target authenticator.

- Two possible approaches to address the context binding issue
  - **Approach 1**: communicating the lower-layer context as opaque data via pre-authentication signaling
  - **Approach 2**: use of normal EAP authentication after handover with using the same link-layer independent context for both pre-authentication and normal authentication
Pre-authentication protocol work in HOKEY WG

- Is there any protocol work needs to be done in this WG?
  - L2-agnostic pre-authentication protocol should be defined in IETF (IETF pre-authentication protocol)
    - PANA WG is defining pre-authentication extension for PANA
    - IETF pre-authentication protocol needs to be aligned with HOKEY WG charter, i.e., it should not attempt to solve authenticator discovery with link-layer address or context binding
  - L2-aware pre-authentication protocol should be defined outside IETF
    - In IEEE 802, Security Study Group is being formed in 802.21 WG
      - Pre-authentication is recognized as one study item
  - Defining new AAA attributes for pre-auth should be done in DIME and RADEXT WGs

- Pre-authentication problem statement and AAA requirements seems to be more important work in HOKEY WG
Conclusion

• Merge draft-nakhjiri-preauth-aaa-req-00 and draft-ohba-preauth-ps-01.txt into a HOKEY WG draft (intended status: Informational)

• No pre-authentication protocol needs to be defined in HOKEY WG
Back-Ups
Basic pre-auth AAA requirements

• Requirements identified in IETF65 HOAKEY BOF
  – AAA needs to know that this is a pre-authentication not normal authentication
    • User may only be allowed to have a single logon at the same time
  – AAA needs to know how long to hold the session before timing out
    • Session timeout for pre-auth may be different for normal session
    • If the mobile moves after timeout then do normal authentication
    • Addressed in draft-aboba-radext-wlan-03.txt

• Other requirements are explained in next slides
Extending pre-auth session lifetime

• Pre-authentication session lifetime may need to be extended
  – The MN may continue to stay in the serving network or move to some other network, while maintaining the pre-authentication session with a target authenticator

• Maximum pre-auth session lifetime may need to be defined in order to avoid unlimited attempts for extending pre-auth session lifetime
Reverting to pre-auth state from full authorized state

• A session with a fully authorized state may need to be changed to a pre-auth state
  – This can happen when MN moves from network N1 to network N2, and it may go back to N1 again
  – MN may not want to perform pre-authentication again with N1
Maximum number of pre-auth sessions for different authenticators

• How many pre-authentication sessions for different authenticators are allowed per MN?

• Is this a AAA protocol issue or a AAA protocol implementation issue?
  – This may be a AAA protocol issue for indirect pre-authentication in which the serving authenticator is involved in pre-auth signaling
Information on the serving network

• AAA server may need information on the serving network from which a pre-authentication attempt is being made
• This information may affect the authorization decision made by AAA server
Calling-Station-Id

• What should Calling-Station-Id be in the case of inter-technology pre-authentication?
  – Should it be the MN’s address used for the serving network?
    • In this case, a Calling-Station-Id may dynamically change if MN handovers to a new nerving network and still maintains the pre-authentication state with the target network
  – Should it be the MN’s address to be used for the target network?
  – Should it be null?
Network-initiated pre-authentication

• Are new AAA attributes needed to support network-initiated pre-authentication?
  – E.g., list of neighboring authenticators around the serving authenticator