EAP Re-authentication Extensions

Vidya Narayanan
Lakshminath Dondeti
IETF-69, Chicago, July 2007
Deltas from 01 to 03

• Deleted references to 11r key hierarchy etc.
• Order of usage of server-id, rIKname (as NAI) and peer-id for consistent now
• Key derivation
  – Removed references to including "other parameters"
  – For this specific usage no other material needs to be added.
• rMSK length
  – HOKEY server may not necessarily know the MSK length.
  – HOKEY keys come from the EMSK and so changed to EMSK length
• rIK length
  – rIK length would not be known at the time of derivation
    • Length set equal to EMSK
  – See discussion on CFRG on the topic
    • Hash to compress the key if needed
Deltas from 01 to 03

• Clarified that cryptosuite does not include the PRF; algorithm agility is provided from the EAP method
• Added clarification text on NAI that goes with rIK name
• Simplified error processing
• Clarified sequence number maintenance semantics
Issue Tracker – Issue #4

• Channel binding in ERX
  – Draft has some text on channel binding
    • Review and comments welcome
Issue Tracker – Issue #5

• Optional authenticator-initiated message
  – Optional EAP Initiate/Re-auth-Start message from authenticator?
  – Re-transmission similar to 802.1x EAPoL-Start message
  – Authenticator to send both EAP Request Identity and EAP Initiate/Re-auth-Start to peers that attach?
    • Authenticators with knowledge of peer possessing valid EAP key material may only send EAP Initiate/Re-auth-Start
Other Open Issues

• DoS attack discussion on the list
  – Issue:
    • Attacker sends ERP Initiate using the rIKName of peer and causes a RADIUS Access Reject to be returned; connection for legitimate peer may be closed
  – Mitigation techniques:
    • When a valid MSK/rMSK is present, the connection is not closed
    • Do not accept unprotected ERP messages from a peer that has a valid TSK
    • Change rIKName across ERP runs
      – This may be desirable for privacy reasons as well
Other Open Issues

• Terminology
  – rRK vs. HRK
  – rMSK vs. something else?
  – Others?
Next Steps

• Address open issues
• Issue WG LC?