HOKEY WG Meeting

IETF 71

Charles Clancy, Glen Zorn

Agenda

- Administrivia, Chairs (5 min)
  - Blue Sheets
  - Agenda Bashing
  - Note Takers
- Document Status, Chairs (15 min)
- Key Management Intro, Chairs (10 min)
- Key Management Document, Yoshi (20 min)
  - draft-ietf-hokey-key-mgm-03
- AAA Support For ERX, Lakshminath (20 min)
  - draft-goankar-radext-erp-attrs-03
  - draft-dondeti-dime-eap-diameter-01
- Key Management Discussion (50 min)
- Pre-auth Problem Statement, Yoshi (15 min)
  - draft-ietf-hokey-preauth-ps-02
- Pre-auth Discussion (15 min)

Working Group Milestones

Date	Milestone
Done	First draft on EMSK-based Keying Hierarchy
Done	First draft with a problem statement on EAP re-authentication and key management
Done	First draft on EAP Re-authentication and Handover Keying Hierarchy
Done	First draft on EAP Re-authentication Protocol
Done	First draft on Protocol and Keying Hierarchy for Visited Domain Handovers and Re-authentication
Done	Submit EMSK-based Keying Hierarchy draft to IESG
Done	First draft on Handover Key Distribution Protocol
Done	Submit the problem statement draft to IESG
Done	Submit EAP Re-authentication and Handover Keying Hierarchy draft to IESG
Done	Submit EAP Re-authentication Protocol draft to IESG
Sep 2007	Submit Protocol and Keying Hierarchy for Visited Domain Handovers and Re-authentication draft to IESG
Done	First draft on EAP Pre-authentication Specification for inter-technology and inter-domain handoffs
Mar 2008	Submit EAP Pre-authentication Specification to IESG

Document Status

- draft-ietf-hokey-reauth-ps-09
  - State: “Approved-announcement sent”
  - IETF LC in February followed by IESG evaluation
  - 08, 09, & RFC-Editor-Note resolved LC comments and two IESG discusses
- draft-ietf-hokey-erx-13
  - State: “IESG Evaluation::AD Follow up”
  - IETF LC in February followed by IESG evaluation
  - 5 new versions to address LC comments
  - Discuss from Jari remains
    - “Truth in advertising” for compatibility with existing deployments

Document Status

- draft-ietf-hokey-emsk-hierarchy
  - State: “In Last Call”
  - IETF LC started February 29, ends March 20
- draft-ietf-hokey-key-mgmt
  - Topic of much of today’s discussion
- draft-ietf-hokey-preauth-ps
  - On today’s agenda
  - WGLC soon?

Key Management Intro

- draft-ietf-hokey-key-mgm
- WG consensus
  - AAA-based transport
  - Support hop-by-hop security associations in key transport
  - Seems consistent with some interpretations of RFC 4962
- Open questions
  - How?
  - End-to-end security support?

Approaches

- Diameter TLS support seems sufficient
- RADIUS shared secret insufficient
  - Even hop-by-hop security requires additional protection
  - Various RADEXT approaches to crypto agility provide necessary protection
    - Keywrap, DTLS, RADSEC
  - Do we depend on TBD RADEXT solution, or do we support/require our own AAA security sublayer?
- To what extent do we want to specify other transports?
  - Other transports have different security properties

Goals

- Upcoming talks outline proposed approaches
- Key WG questions:
  1. Do we want to reuse TBD RADEXT crypto agility solution to provide transport security for key distribution?
  2. Do we want to include support for our own confidentiality and integrity protection?
     - Somewhat orthogonal to #1, as we may want to support it regardless for other transports
  3. Do we want to include optional support for end-to-end security?
  4. Do we want to specify/support any other transports? If so, where?
     - Would require discussion of the necessary properties for acceptable transport