HOKEY WG Minutes
IETF 73
Wednesday, November 19, 2008
0900-1015, Salon E

AGENDA

0900-0915: Administrivia, Document Status (Chairs)

0915-0930: Preauth Document Discussion (Zorn)
draft-ietf-hokey-preauth-ps-04

0930-1015: Key Management Document Discussion (Dondeti/Narayanan)
draft-ietf-hokey-key-mgm-04

MINUTES

0900-1915 – Administrivia, Document Status (Chairs)

Welcome, Secretary (Dorothy Stanley), Jabber scribe (Name), blue sheets Current RFCs

- Reauth Problem statement
- ERX
- EMSK Keying Hierarchy

In Progress

- Preauth problem statement
- Key Management DOC

0915-0920 Preauth Discussion document, draft-ietf-hokey-preauth-ps-04

- Glen – the document has been revised and improved
- Have a few comments, include in the IETF last call

0920-0935 Status of Key Management document- Vidya Narayanan

- Merged with draft–goankar-radext-erp-attrs
- Put focus on distribution of USRK, DSRK and USDSRK over RADIUS, relying on RADIUS Security
- Removed “three party”
- Revised security requirements section.
- Description of Basic Key Distribution Exchange (KDE) Sequence
- Description of Combined KDE sequence for distributing DSRK and DSUSRK
- Description of RADIUS KDE Attribute
- Description of when and how the KDE Attribute is carried, Explicit and Implicit

ERP Bootstrapping

- Summary of Security Requirements on RADIUS Key Transport
- Glen: Does the document require that the entire RADIUS message be encrypted?
- Vidya: KDE attribute must be encrypted. Not adding new requirements on RADIUS.

- Requirements on hop-by-hop requirements
- Security Consideration on Lack of Peer Consent
- Still work to do to clean up drafts, simpler explanations, uniform use of terms
- Katrin: The use of “three party” was removed, but “third party” terms still in the draft
- Vidya, Charles – Might need a better term, USR-KH, three party is different than third party.

0935-0940 Status of HOKEY Key Distribution Exchange document – Charles Clancy

- Crypto protocol no longer present
- Go through sections 3 and 4 to condense and reduct text to what is needed; no longer specifying a crypto protocol
- Section 7 describes security considerations
- Plan between now and the next meeting is to clean up sections 3,4 get review from the WG on sections 5,6,7
- Then should be done with this document (and all our documents)

0940-0945 Discussion

- Vidya: Are we shutting down as a WG?
- Glen: in addition to re-reviewing this document at the next meeting, we’ll discuss re-chartering
- Vidya: Is there an interest in rechartering
- Glen: We haven’t asked for input on rechartering yet. There have been issues raised in our documents that need solutions. e.g. modifications to IKEv2, investigate if changes needed to 802.1X
- Would the IKEv2 changes go here, or in another groups
- Tim Polk: Greatly appreciate the chairs’ focus on current work items to finish. Not opposed to the group rechartering, if there is energy, work. Consider in San Francisco. There have been open issues that we have had to punt on as we were going through. Revisit those here, reasonable plan
- Glen: Are there any other items to discuss?
- Glen: None, we’re done.