The HIP Diet Exchange
HIP DEX

Robert Moskowitz
Verizon Telcom and Business
Innovation Group

March 29, 2011

rgm@labs.htt-consult.com

Purpose of this presentation

- An update on HIP DEX progress
  - Status of Draft
  - Issues with new HIP Parameters
  - Implication of 'loss' of HIP Packet signing
    - Only MACing available
  - Next steps

Status of HIP DEX?

- Draft updated – 05.txt
  - An another in the pipe
- Need to reconcile common text with 5201-bis
  - Many paragraphs to review
- Need review of KDF function based on CMAC
  - E.G. Additional info part of extract phase which is not included in draft SP800-56C
- Need to solidify HIT derivation
- Need additional review
  - Welcome a co-author

Status of HIP DEX?

- Added Pair-wise and Group Security Association management
- HIP generated keying material ONLY used to protect HIP packets
  - Increases longevity of keying material
- Key wrapping of 'session' keys
  - Need review of wrapping

Issues with HIP Parameters

- A number of new Parameters
  - Variants/replacement for BEX Parameters
  - Frequently the same function but MACing replacing SIGNing
  - Is text needed to explain this phenomenon?
  - Type assignments?

Implication of loss of SIGNing

- DEX does NOT provide for SIGNing
  - SIGNing REQUIRES a Cryptographic Hash
    - Existential Forgeries
- Replacing SIGNing with MACing results in
  - Loss of non-repudiation
- Managed in Base exchange
- Major impact to UPDATE packets
  - Note that UPDATE packets are now used to distribute pair-wise and group keys

Next Steps

- CORE
  - CORE is the application protocol for sensors running over 6lowpan
    - Basically a subset of HTTP
  - CORE has selected DTLS for their security protocol over ESP, as the app has direct knowledge of the presence or lack of security
  - If certificates are supported in the sensor, then EAP-TTLS will be used for the KMP
  - If no certificates then DTLS-PSK will be used
  - CORE MUST specify a KMP for DTLS-PSK

Next Steps

- CORE
  - Work on CORE bootstraping of DTLS PSK using HIP DEX
  - More an issue of how to use HIP in general for CORE bootstraping
    - 'Mother-Duckling' model
    - HIP Rendezvous server as the 'Mother'?
    - HIP Registration using DEX limitations?
      - Add this into HIP DEX draft or separate document?
  - If selected by CORE will require HIP DEX to be Standards track
  - Looking for participants in CORE
    - A couple already

Next Steps

- IEEE 802.15.4
  - 802.15.4 has a MAC security framework, but specifies the KMP as 'out of scope'
    - But still needs one
  - Zigbee specifies PANA EAP-TTLS for KMP
    - This is recognized as 'too big' for many sensors
  - Desire for a KMP that will work on battery powered, constrained, sensors

Next Steps

- IEEE 802.15.4
  - Addendum 15.4e adds Information Elements to 15.4
    - Basically a TLV in management frames
  - Using IEs can make adding HIP DEX for 15.4 KMP a 'recommended practice' document, not an addendum
  - Need to deal with HIP packets carried over a set of 15.4 management frames
    - This actually is a broader issue in 15.4g

Questions?