The HIP Diet Exchange
HIP DEX

Robert Moskowitz
Verizon
Innovation Group

November 17, 2011

rgm@labs.htt-consult.com

Purpose of this presentation

- Why HIP DEX
- An update on HIP DEX progress
  - Status of Draft
  - Next steps

Why HIP DEX

- VERY Constrained Devices 'resist' Key Management
  - At best rely on static secret as Asymmetric Cryptography too expensive
- ECDH His
  - 'Only' need wide multiply
  - Static ECDH
    - Only Crypto function added to devices
      - Have AES-CCM in Layer 2
  - No signing
    - No Crypto Hash
  - MACing only
    - CMAC
    - KEYmat via CMAC as well

Implication of loss of SIGNing

- Replacing SIGNing with MACing results in
  - Loss of non-repudiation
- Major impact to UPDATE packets
  - Note that UPDATE packets are now used to distribute pair-wise and group keys

Status of HIP DEX?

- Draft update in progress – 06.txt
- Still need to reconcile common text with 5201-bis
- Change from AES-CBC to CTR for Encrypted_Key
- 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 review of Key wrapping of session keys

Next Steps

- IEEE 802.15
  - New PAR, 802.15.9, will provide 'shim' for transport of KMP datagrams
    - This is KMP agnostic
  - Mandates using 802.15.4e Information Elements
  - Use cases and guidelines for using HIP (both BEX and DEX) for 802.15 KMP
  - Work starting in Jan '12

Next Steps

- 6lowpan
  - Draft for Dispatch ID for 802.15.9 KMP shim
    - For pre-4e devices
    - 'Port access' control may be a little complex on 4e compliant controller
      - Both 4e and pre-4e sensors in PAN

Next Steps

- CORE
  - 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
    - No specification of source of PSK
  - Adding TLS-Rawkey
    - Sound familiar?

Next Steps

- CORE
  - Minimally develop ID for using HIP DEX as source of PSK for DTLS-PSK
  - And/or develop ID for HIP DEX for use with DTLS datagrams
    - Maybe not too hard to do for sensor
    - But may be really hard to do for server

Questions?