Interconnecting Smart Objects with Internet Workshop 2011-03-25

IKEv2 and Smart Objects
Tero Kivinen <kivinen@iki.fi>
AuthenTec
draft-kivinen-ipsecme-ikev2-minimal-00.txt
Example Use Case

- Garage door opener
  - Two buttons:
    - one to unlock and open door
    - another to close and lock the door
  - One led for feedback
  - Uses two-way radio communications
  - Obviously needs some kind of security
  - Battery powered
Example protocol

• Protocol can be very simple:
  – Send packet to server to start open/close door
  – Get packet back to acknowledge the command
  – Get status messages every second while door is moving
  – Get final message when operation is done

• Simple way would be to use WLAN / IP / UDP for communications

• Requires security
  – DTLS, Ipsec/IKEv2, proprietary
Protocol effects

- Device only wakes up when button is pressed
  - It always initiates the communication, it does not need to listen radio when it is sleeping, and it cannot reply to any messages while sleeping.
- Device stays awake for some time after the button is pressed and if receives status packet blinks led and waits for more status packets.
- After certain timeout device goes back to sleep
What this means for IKEv2

- Device only needs work as IKEv2 Initiator
  - No need to work as IKEv2 Responder
- Only creates one IKEv2 SA and one IPsec SA
  - No need to support SA management operations like creating new IPsec SAs, rekeying, deleting SAs, etc.
- No need to do NAT-T, Configuration payloads, EAP authentication, Cookies, Multiple child SAs etc
- The server end would most likely be some kind of Home area network server (PC or similar).
- Pre-shared keys or RAW RSA keys authentication
  - No X.509 certificates
Authentication

- **Pre-shared keys**
  - Shared key printed on paper or in electronic form
  - Typed in to the home area gateway
- **Raw RSA keys**
  - Fingerprint of device is distributed as Pre-shared keys
  - Device imprints to first home area gateway it connects to
  - Some form of reset can be implemented to allow reimprinting
I created a prototype implementation of the minimal IKEv2 protocol usable for such scenarios and it took me less than a day to write the code and less than 1000 lines of perl source code.

- I implemented sending ICMP Ping packet as didn't want to start writing server end to answer my requests...

Implementing minimal IKEv2 is very simple compared to full implementation.

There are some optimizations which can be done when only supporting minimal set of features.
Conclusions

- IKEv2 is very small protocol when only minimal features are implemented
  - Not sure whether TLS / DTLS can be made that small
  - Our full IKEv2 implementation is 44k lines
- Certificate support would multiply the code size
  - Our certificate library is 56k lines or 81k lines if enrollment and CRL retrieval protocols are included.
- Pre-shared keys or RAW RSA keys are feasible options for authentication in this kind if use scenarios
- My draft describes those optimizations needed:
  - draft-kivinen-ipsecme-ikev2-minimal-00.txt