PAWS: Security Considerations

draft-wu-paws-secutity-01

Yizhuang Wu, Yang Cui

IETF 85@Atlanta, 2012-11-08

Motivations

- Focus on the security countermeasure
  - Following the security requirements in WG doc
- To provide an informational guide for security design of PAWS
  - Mutual authentication
  - Regulatory body model
  - Crypto channel binding
  - Pre-shared Key and Certificate
  - Protection of credentials on device

Why presentation here?

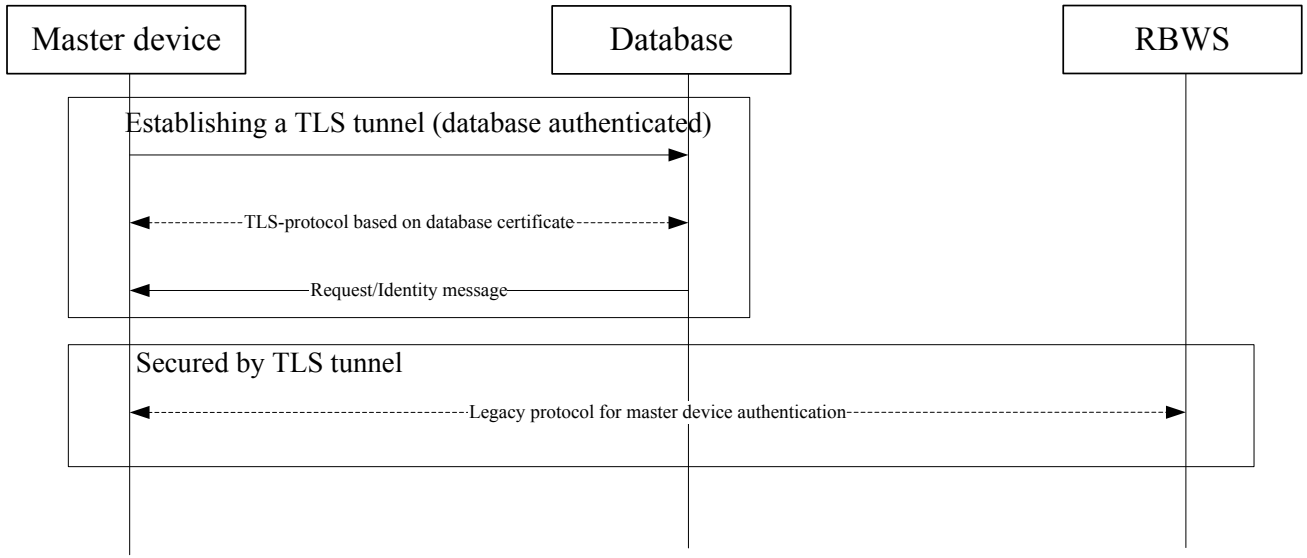
- -00 version before Vancouver meeting
  - Point out channel binding problem on the list and a couple of email discussion
  - Lots of discussion on security at Vancouver
  - Not enough time to present at Vancouver
- -01 version
  - Simplify auth models
  - Limitation of TLS
  - Minor revision

This draft

- Include, but not restricted to
  - Against MitM attack (channel binding)
  - Against physical attack to master device (secure module like TPM)
  - Authentication w/t, w/o RBWS
  - etc…
- If WG considers the security issues should be dealt with

Such as, authentication with RBWS

- The credentials of master device shall be authenticated by RBWS through the TLS secure tunnel or in procedure of the TLS handshake protocol. The authentication procedure using mix mode is depicted as follows:



Thank you