IDevID vs LDevID

Charles Qi
Broadcom Corp.
July 19th, 2006

Goals

- Draw comparison on the TPM usage model of identity keys vs. 802.1ar usage model of identity keys

BROADCOM
Connecting everything

The TPM Usage Model

- TPM have sophisticated usage models on credentials and keys that can be used as identity of the device
- TPM defines an endorsement key (EK) which is physically bond to the device (embedded), EK is effectively an RSA private key/public key pair
- The usage of EK is restricted to only establishing the ownership for the TPM, where the owner authorization data is protected by EK-encryption
- The EK credential is typically issued by the TPM manufacturer, disclosure of the EK credential reveals the identity of the TPM
- AIK is created for privacy protection, AIK credential can be issued by CAs vouching the AIK is bond to a valid TPM without disclosing the identity of the TPM
- AIK can only be created by the TPM owner

BROADCOM.
Connecting everything®

Comparison of TPM vs. 802.1ar

- The 802.1ar IDevID is close to the TPM EK, the 802.1ar LDevID is close to the TPM AIKs
- The 802.1ar doesn't explicitly define the ownership, so the creation of the LDevID (enrollment) is not as secure as the creation of AIK in TPM
- The EK TPM is never used as a signature key, in this regard, it is probably not exactly what is intended for IDevID
- The AIK is much more close to what is intended for LDevID

BROADCOM
Connecting everything

The 802.1ar Usage Model

- It doesn't seem to be correct if we just borrow the TPM EK/AIK model for IDevID/LDevID
- It might make sense to limit the IDevID only to the provisioning of the LDevIDs, unless the LDevID is never provisioned
- To put it differently, once the LDevID is provisioned, the IDevID SHOULD not be used directly in a generic authentication other than for the purpose of provision new LDevIDs
- There are two problems to solve if we want to distinguish the usage of IDevID vs LDevID
  - The is no enrollment procedure defined to restrict the usage of IDevID to only that
  - There is no way to differentiate between IDevID and LDevID by just examining the certificates associated

BROADCOM
Connecting everything