Signer ID Retrieval Design
Agenda

• Quick recap
  • Authentication Mechanism
  • Role of public key
• What is signer ID and its usage?
• Design of signer ID retrieval for attestation
Authentication Mechanism

1. Load Key Certificate
   - Authenticate the key using the parent public key
   - Save the public key
   - Parent public key either of -
     1. Previously authenticated in CoT
     2. Verified ROTPK

2. Load Content Certificate
   - Authenticate hashes using the saved public key
   - Save the Hashes

3. Load Image
   - Calculate the hash of the image and compare against saved one
   - Image is authenticated
Authentication Mechanism

- **Signer**
- **ROTPK**
  - Load Content Certificate
  - Authenticate hashes using the saved public key
  - Save the Hashes

- **Calculate the hash of the image and compare against the saved one**
  - Image is authenticated
What is signer ID and its use?

- The hash of a signing authority public key for the software component.
- Due to the fact that boot certificates are not measured, the Signer-ID must be taken into account when attestation is carried out.
- Signer-ID can be used by a verifier to ensure the components were signed by an expected trusted source.
- Signer-ID enables fine-grained policy-based decisions, ultimately determining platform approval.
Design of Signer-ID retrieval

• The Authenticated Public Key (Signer) of an image is retrieved during authentication as discussed previously.

• The platform can measure the key using the Crypto Module via "plat_mboot_measure_key".

• Moreover, platform can pass that measurement to appropriate Measured Boot backends such as RSS or Event Log for extending measurements.

• Measurements are provided to an external verifier, who then can use them to unseal some security policies, eventually helping to attest the platform. This is platform IMPDEF.
References

• Patches posted externally for review -
  • https://review.trustedfirmware.org/q/topic:%22mb%252Fmb-signer-id%22+(status:open%20OR%20status:merged)

• Signer ID details -
  • https://arm-software.github.io/psa-api/attestation/1.0/IHI0085-PSA_Certified_Attestation_API-1.0.3.pdf
Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
ありがとう
Asante
Merci
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה