Digital Display Test Slide

Stay tuned for the following Feature Presentation

by Landon Curt Noll

chongo@cisco.com

Key Management Policy
a proposal for a policy model

Landon Curt Noll

chongo@cisco.com

Version 0.3

Policy Objects

- Identified by a SOGUID
  - Special SOGUIDs that start with -- for standard defined policies
- Referenced by another security object
  - Meta data of security object (i.e., key, client, etc.)
- Provides information related to an action
  - Informs an actor (i.e., KM Client, KM Server, etc.) of policy details

Policy Objects are NOT code

- May require an actor to execute code
  - An actor will likely execute code to perform the policy
- May contain meta-data that helps the actor perform
  - Policy specific meta-data parameters

Key life cycle actions

- Enforced by the standard
- Not a policy
  - e.g., disabling a key after based on a disable timestamp is not enforced by policy
- Policies deal with Key Management Exceptions

Policy Objects contain

- Human readable name
  - The policy object is referenced by SOGUID
- Enforcement level
  - Mandatory, Important, Optional
- Scope of the policy
  - who will carry out the policy
- Policy Meta-data
  - Parameters for actors carrying out the policy

Policy enforcement - mandatory level

- Must fail the KM op on policy error
  - e.g., an action does not know how to carry out a policy
- Client scope: KMS verifies KM Client is certified
  - based on information attached to the client security object
    - *details initially established when the client is enrolled into the KMS*
- KMS scope: KM Client verifies KM Server is certified
  - based on information returned by KM Server at client login
    - *KM Server may have to tunnel op to another KM Server*
- Logging
  - Logging of both success and failure by actor is mandatory
    - *when actor is in scope*
- Useful when policy is absolutely critical

Policy enforcement - important level

- Policy failure does not require the KM op to fail
  - Perform action on a best effort
  - An actor is allowed to fail KM op, but is not required
- Client scope: No need to verify KM Client
- KMS scope: No need to verify KM Server
- Logging
  - Logging of a policy failure by actor is mandatory
    - *when actor is in scope*
  - Logging of policy success is recommended
    - *when actor is in scope*
- Useful when performing the op is more important

Policy enforcement - optional level

- Policy failure shall not result in KM op error
  - Perform action on a best effort
- Client scope: No need to verify KM Client
- KMS scope: No need to verify KM Server
- Logging
  - Logging of a policy failure/success by actor is optional
    - *when actor is in scope*
- Useful for debugging and tracing

Policy Scope

- Determines the actors for whom the policy applies
- KM Clients identified by SOGIUD
- Special scopes
  - SOGUID that starts with a --
  - --KMS
    - *Applies to the KM Servers in the KMS*
  - --KMClient
    - *Applies to any client*
  - --KMClient.domain
    - *Applies to KM CLients in a given domain*

Policy scope list

- List of SOGUID of scope & Enforcement level
- Ordered list
  - First match applies

Policy Meta-data

- Binary blob with scope
- Meta-data Scope
  - Determines which actors should pay attention
  - Same syntax as policy scope