Key Management Challenge, Issues, and Scale

How to make Encryption Management operationally relevant

Agenda

- Technical Requirements for Encryption Management
- Constraints (NIST 800-57, FIPS 140-2, NIST 800-130, NIST 800-152 Draft 3)
- Key Material, Operations, and Attributes
- Functionality in Key Management
- Performance in Key Management
- Interoperability in Key Management
- Security in Key Management
- Attributes and Scale
- Rules, Policies, and Attributes for Encryption Key Management
- Applying Security Concepts to Encryption Key Management: Attribute Based Access Control

SEMPER FORTIS SOLUTIONS

FORNETIX

Technical Requirements for Encryption Management

- Problem Space
  - System: The need to manage encryption keys for communications for networks, users, and communication devices
  - Physical: The need to manage encryption keys in storage and other endpoints
  - Logical: The need to manage encryption keys for Processes, Files, and Objects
- With more network aware technology the distinction of System, Physical, and Logical becomes blurred

Constraints

- Besides common sense (keys need to be accessible and secure) what constraints are there for Encryption and Encryption Management:

- NIST SP800-57: Recommendation for Key Management
  - Dictates Encryption Key Lifecycle
- FIPS 140-2 : Security Requirements for Cryptographic Modules:
  - Specifies the nature of encryption and ciphers
- NIST SP800-130: A Framework for Key Management Systems
  - Specifies the nature of encryption key management
- NIST SP800-152: (DRAFT) A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS) (Third Draft)-
  - Specifies the Federal Profile for Encryption Key Management

Key Material, Operations, and Attributes

- When looking at Key Management and Key Lifecycle the following need to be considered
- Key Material – What you are actually managing– Symmetric Keys, Asymmetric Keys, Spilt Keys, etc. (the information being managed)
- Operations – What can be done with the Key Material (Create, Get, Find, Revoke, Delete, etc.)
- Attributes – How do you describe the key material – Key Length, Validity period, Utilization specific
  - That last category is crucial and helps define how Encryption Keys are used in the System.

Functionality and Key Management

- Given that Keys are metadata associated with information – the use of the information is only relevant insomuch as it is related to understanding the workflow in which encryption management is invoked.
  - Key Lifecycle in regards to utilization defines Functionality for Key Management
- Simply put – no one goes to work to use encryption, they use encryption to go to work: act accordingly.
  - Encryption Management needs to be able to facilitate using encryption.
- With that understanding, what is important for encryption management is the non-functional quality attributes of Performance, Security and Interoperability

Performance and Key Management

- Key Management for System level activities (Session Authentication, IPSEC, etc.) is driven by AVAILABILITY of Key Material in light of the System level component using Key Material

- Key management for physical and logical components (Processes, Storage, File, Object Encryption) is driven by both AVAILABILITY and PERFORAMCE of the Key Material
  - Users have an expectation that the impact of encryption is transparent.

Addressing Performance

- Much like Utilization of Encryption the Creation of Encryption Keys also impacts system performance at Scale.
  - Remember that creating a AES Key and Using an AES Key are two different things.
  - Variation in Ciphers and Algorithms also demonstrate changes in performance (Making and Using Asymmetric Keys is more computationally expensive then using Symmetric Keys)
- Key Management Systems need to Queue known Encryption Key types based on System, Physical, and Logical Implementation
  - In practice a given Key Management system can build queues of keys for various types of transactions
- Key Management Systems need to have a logical means of determining when to release a queued Key vs create a New Key on the fly
  - It is important to note that it is more effective to provide a key that is already created vs creating a new one.
  - This does not impact the cost of using the key, but it does reduce the cost of creating the key
  - Being able to categorize key material in light of Attributes is one way to facilitate release of key material

Interoperability and Key Management

- Once used, encryption management represents the keys to the kingdom both figuratively and literally
- In enterprise systems Interoperability represents protection against system brittleness driven by functionality, security, and performance
  - Only focusing on making it work quickly and securely can have serious negative impacts if how it communicates is not consistent – especially at scale.

Addressing Interoperability

- In a word… Standards
  - KMIP, SAML, PKCS11, XACML etc.
- When considering the data contract for systems components associated with Encryption Management it is essential to look at standards associated with not just Encryption Management but the services associated it with it.\
  - When designing high performance systems it is important to consider how the sub systems components communicate and if there is a standard that covers the communication.

Security and Key Management

- Much like Authentication and Authorization protecting Keys is similar to protecting Identity
- Managed keys need controlled Accessibility
  - This means known protocols with understood security mechanisms
- In practice invoking key release takes on the same nature of behavior as asserting identity for authentication, or asserting authenticated identity for authorization

Addressing Security

- Given both system and user requirements for encryption management it is important to support both device and user credentials in encryption management transactions
  - Username/password, nonce, OTP, link level credentials, etc.
- Given the use of standards, it is important to implement safeguards to protect the standards just like any other enterprise service
  - Communication between any two systems is vulnerable if controls are not implemented
- The concept of attributes for key material opens up interesting doors for addressing Authorization in both releasing key material but (more importantly) in using key material

Attributes and Scale

- Encryption Management happens regardless of method of encryption
- Method of encryption, cipher etc. can directly impact storage performance in terms of IOPS
- Encryption management complexity and performance is driven by network, and scope of encryption of the system
- Scope of encryption management in terms of storage relates to how to communicate with the storage, how the storage protects the information, and if processes that use the storage use encryption and an additional security control
- The number of methods for using encryption plus the amount of information, and the type of information drives the number of attributes associated with the encryption key material being managed

Rules, Policies, and Attributes

- With an ability to catalog managed Key Material via Attributes this opens doors for addressing policy not just within Key Management but also external handing of attributes
- Attributes can be specific to key management (IE State, Protect Start, Protect Stop) or they can specific to utilization of the encryption Key (SSH - comms, Project Banana - DoDIC, Knee condition - HIPAA)\
- Key Management systems need to be to categorize rules and policy around attributes for internal workflow
- The messages originating from Key Management need to address attributes to inform external workflow in which Key Management is invoked
  - Consider it Orthogonal Networking
- Rules and Policy become decisions based on attributes defined by the users of the system that is leveraging Key Management

Attributes and Attribute Based Access Control (ABAC)

- Being able to categorize attributes associated with Key Material allows developing rules and policies around those attributes
- This lends itself towards fine-grained or attributed based access control associated with the creation/release/lifecycle of key material
- ABAC as a System feature provides a mechanism to coordinate authorization through System, Physical, and Logical components.