Key Management

The Key to Secure Storage

Michael Willett
Seagate Technology
Trusted Computing Group
Overview

- Basic Key Types
- Uses of Keys
- Key Management
- Standards Organizations
Keys
Key Uses

- Private signature key
- Public signature verification key
- Symmetric authentication key
- Private authentication key
- Public authentication key
- Symmetric data encryption key
- Symmetric key wrapping key
- Symmetric and asymmetric random number generation keys
- Symmetric master key
- Private key transport key

- Private signature key
- Public signature verification key
- Symmetric authentication key
- Private authentication key
- Public authentication key
- Symmetric data encryption key
- Symmetric key wrapping key
- Symmetric and asymmetric random number generation keys
- Symmetric master key
- Private key transport key
Basic Key Types

- Data Encryption Keys
  - Symmetric Keys
  - Long Key Lifetime
  - Loss of Key is Loss Of Data
  - Secure Erase
  - Audits
Basic Key Types

- Key Encryption Keys
  - Used to Securely Transfer Data Encryption Keys
  - Ephemeral
  - Asymmetric: Public Key Infrastructure (PKI)
Access Key

- Lock Key
- Authentication
- Drive Needs a Key for Any Access
  - Read Operations
  - Write Operations
- Configuration
Authentication

- Drive Authenticates Host
- Host Can Authenticate Drive
Secure Messaging

- Drives Agree on Encryption Key
- Commands and Data To/From Drive are Encrypted
- Data In Flight (DIF)
Data Encryption Key

- Used to Encrypt/Decrypt Data on Media
- Data At Rest (DAR)
Threats
Disclosure

- Confidentiality
  - Key Disclosed to Unauthorized Entities
  - Data Accessible by Anyone
  - Authentication Failure
  - Eavesdropping
  - Improper Policies and Procedures
Denial of Service

- Integrity
  - Key has Been Modified
  - Data Accessible by None
- Archive
  - Key has Been Lost
- Availability
  - Key Cannot be Accessed
Key Management
Key Servers

Key Server → Key Request → Host → Secure Disk

Key Server → Key Response → Host → Secure Disk
Key Management

The diagram illustrates key management in a storage environment. It shows the flow of key management protocol between the host, array controller, and key servers in domain A and domain B. The protocol ensures secure data transfer and management across these domains.
Standards Organizations
TCG Key Management

- **Key Management Services Subgroup (KMSS)**
- **Define Best Practices for Key Management**
  - Mechanisms to Define and Manage Keys
- **Support for Any Device using the TCG Storage Specification**
  - A Uniform Way to Manage Keys for a Variety of Storage Devices
- **Application Support**
  - Ease Development with a Key Management Application Note
TCG Key Management Operations

- KMSS Addresses Operations Between
  - Host Platform
  - Application
  - Trusted Devices

- Levels of Interaction and Security
- Requesting Key Generation
- Key Usage
- Storage of Keys
- Retrieving Keys
- Modifying Keys
- Searching for Keys
- Key Access Rights
- Disabling of Keys
- Destruction of Keys
TCG KMSS Application Note

- Secure communication between the storage device and the host system.
- Authentication between the storage device and the host system.
- Discovery of the storage device capabilities.
- Compliance with existing data security regulations
- Flexibility to comply with future state and federal legislation.

https://www.trustedcomputinggroup.org/groups/storage/
TCG Future Application Notes

- Key Management for Tape Systems
- Key Management for Optical Storage
- Key Management for Consumer Devices
- Any Application of the TCG Storage Specification
IEEE P1619.3
Questions
More Information

- ISO/IEC 11770 Parts 1-3: Information technology - Security techniques - Key management
- Trusted Computing Group (https://www.trustedcomputinggroup.org/home)
More Information

- IEEE P1619.3: Security in Storage Workgroup (SISWG) Key Management Subcommittee (http://siswg.net/)
- OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi)