Storage Security Using Cryptographic Splitting

David Dodgson

Unisys

Objectives

- Learn about cryptographic splitting: what it is, and how it can be used.
- Learn how splitting can be combined with other encryption methods to provide strong data protection.
- Learn how a storage appliance using these methods can be used to provide secure, highly available access to data.
- Learn how a storage appliance can be used to limit access to data to members of a community of interest at less cost than traditional methods.

Cryptographic Splitting

- Cryptographic splitting is an algorithm that splits a stream of bits into N shares
  - Splitting is done at the bit level
  - Splitting is controlled by a key
  - Splitting is performed randomly

Video on Cryptographic Splitting

- "Stealth for SAN" video at http://www.unisys.com/unisys/ri/videos/index.jsp?id=1200002

Strong Data Protection

- A combination of algorithms is used to provide strong data protection.
  - AES-256
    - A block of data is first encrypted
  - Cryptographic Splitting
    - The encrypted bits are then split into N shares
  - SHA-256
    - Each individual share is hashed

Keys

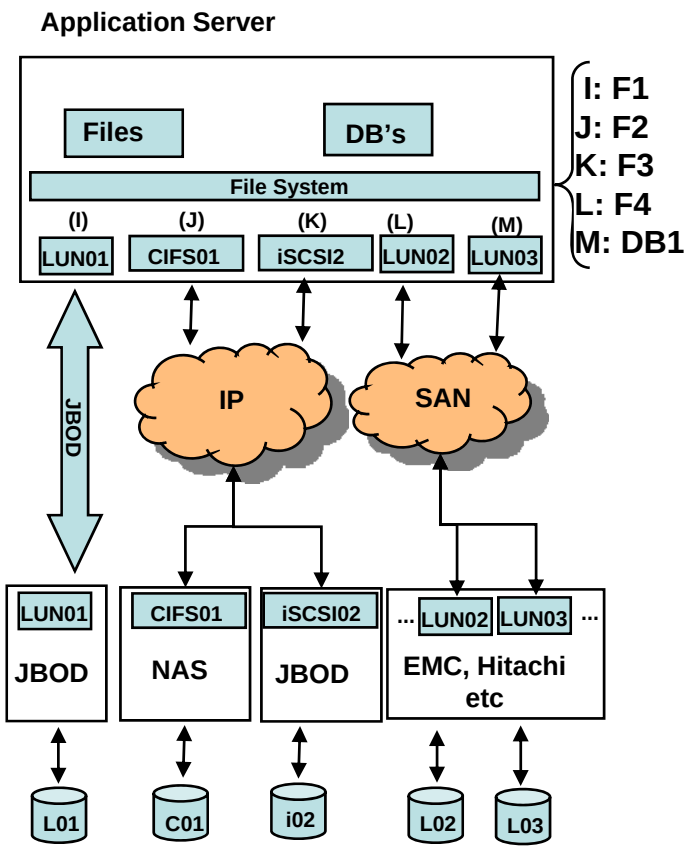
- Workgroup Key
  - External
  - Symmetric, 256 bits
- Session Key
  - Internal
  - Contains encryption, splitting, and hash keys
  - Encrypted with the Workgroup key
  - Used on no more than 64GB of data

Storage Using Splitting

- Data is encrypted and split into N shares
- Each share is saved on a separate disk
  - The loss of any one disk cannot compromise the data
- A storage appliance in the SAN performs the encryption
  - The appliance has a hardware assist to improve performance

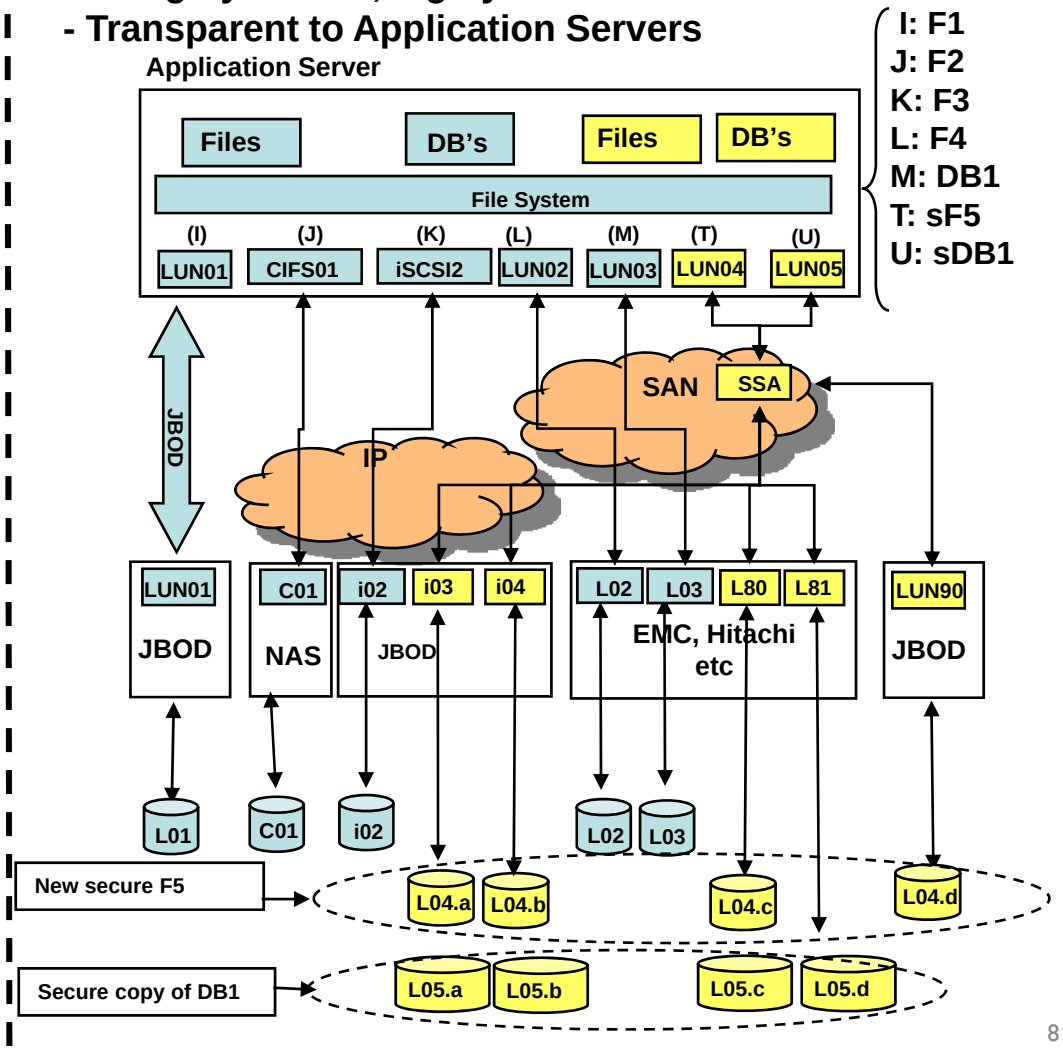
SAN Configuration

Existing Storage Enterprise



SSA enabled Storage Enterprise

- Encrypted data "shred" across multiple physical locations
  - o Highly secure, highly available
- Transparent to Application Servers



Storage Pools

- A Storage Pool is a collection of storage shares
  - For example, four disks could be used where the data is split into four shares where the back-end storage is disks
  - Or, each back-end share could be from a RAID'ed array
- Shares should be distributed across the data center
  - Reduces loss through theft or attack
  - Reduces loss through failure (different circuits and sprinklerheads)

Storage Volumes

- A Storage Volume is storage allocated for a specific use
  - The volume is presented as a virtual disk to a client.
  - It is allocated from a storage pool.

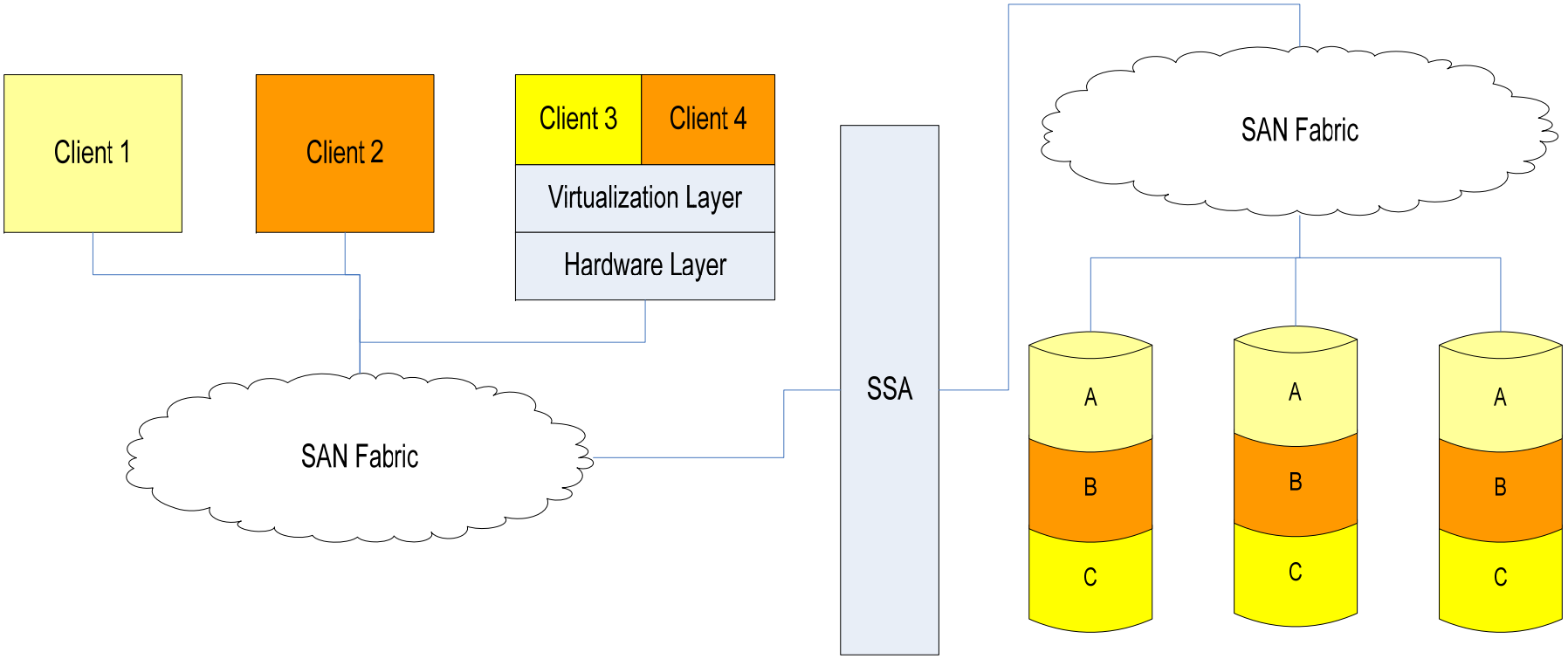
Secure Volumes

- Volume storage is protected by encryption
  - Each volume has a single workgroup key
  - A volume may have multiple session keys, depending on size
- Volume access is protected by masking
  - A volume is only visible to configured external ports
  - I/O request from unconfigured ports are ignored

Communities of Interest

- Storage may be configured for a specific community of interest
  - Each volume has a key specific to its community
  - Access can be restricted to only the application server that needs it
  - The size of the volume is configured to be only what is needed
  - Multiple volumes may be allocated from a single storage pool

COI Example



Redundancy

- The splitting algorithm provides redundancy
  - Specified as "M of N" where N is the number of shares and M is the minimum number required
    - For example, "2 of 4" means that data is written to 4 shares, but only 2 reads are required to reconstitute the data
  - Provides multi-location protection
    - For example, 2 shares could be local and 2 remote
  - Provides multi-layer protection
    - For example, RAID 5+0 could use 4 of 4 to provide striping at the appliance talking to 4 storage devices providing RAID 5

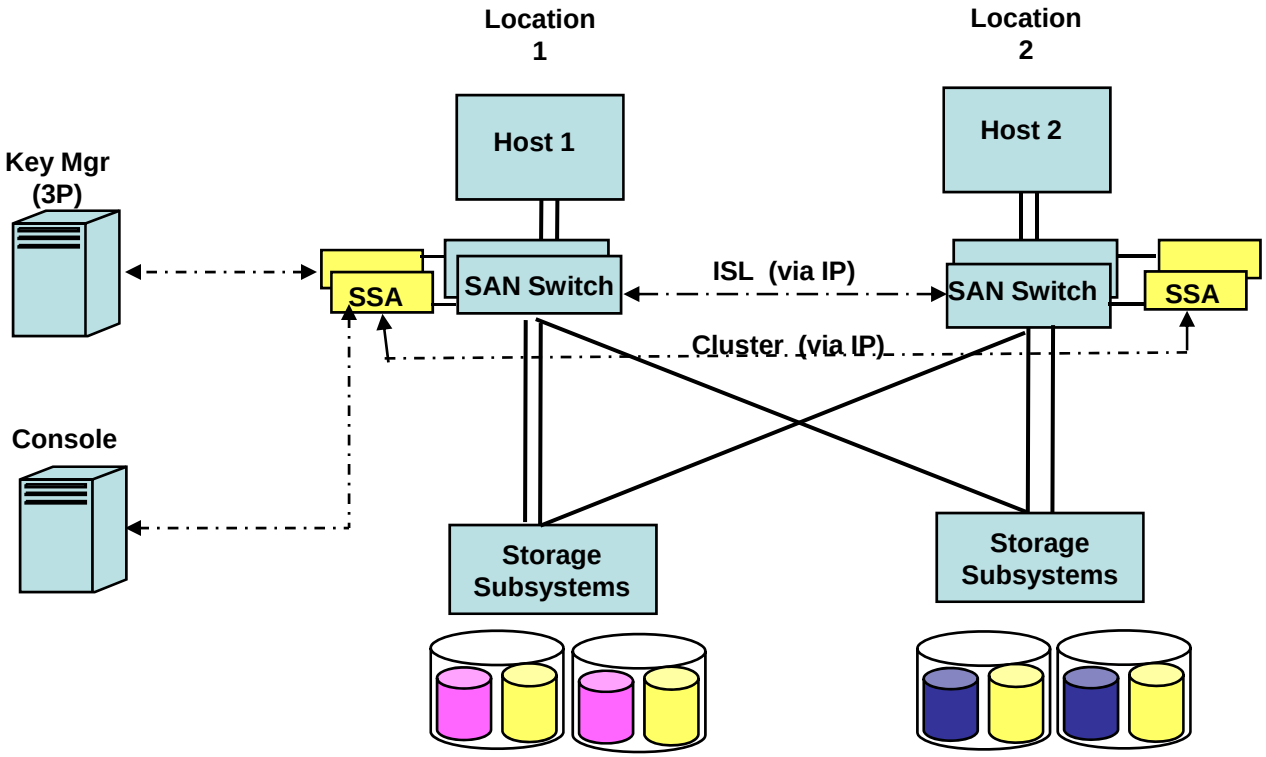
Error Handling

- Various errors can be detected and handled
  - I/O error
    - Probably due to missing share, rebuild later
  - Bad SHA result
    - Probably due to transmission error or data corruption, retry or rebuild
  - Bad merge result
    - Probably due to out-of-date share, rebuild
  - Bad decryption result
    - Probably due to bad data, rebuild
- Rebuild is done automatically when a share's devices return to service

Disaster Recovery

- Multi-pathing
  - An application server may access data through multiple paths
  - The appliance may do the same
- Geographic dispersal
  - As long as at least M shares are available at any location, the data is available
- Clustering
  - Appliances can be combined in a cluster to protect against failure and improve performance (hot/hot)

SAN Network



Rekeying

- Workgroup key
  - Rekey the session keys
- Session keys
  - Rekey the data, one session key at a time
    - Use the old key to access data while rekeying is performed in the background

Caching

- Front-end
  - Recently accessed data can be saved on the appliance
    - Data doesn't have to be decrypted
    - Primarily improves read performance
- Back-end
  - Data for remote shares can be saved locally
    - Saved in encrypted format
    - Primarily improves write performance

Advantages

- Data is protected throughout the SAN
  - Data is safe from eavesdroppers
- Multiple shares
  - No single disk has all the data
- Virtualization and encryption provide COI's
  - Multiple COI's on a disk provide more efficient use of storage
- Data encrypted with a single key is limited
  - No more than 64 GB encrypted with a key

Advantages

- Safer redundancy
  - RAID-5 algorithm provides additional information to attackers
- Centralized key management
  - The appliance can access key life-cycle management
- Improved access
  - Rekeying and rebuilding are done in the background
- Improved performance
  - Using hardware assist

Disadvantages

- Greater complexity in the SAN and configuration
- Redundancy algorithm more storage intensive

Summary

- Cryptographic splitting allows blocks of bits to be randomly split into different shares.
- Combining splitting with standard encryption methods provides a very strong form of data protection.
- A storage appliance can be used to provide high availability, and secure access to data in a SAN by members of individual communities of interest (COIs).

Links

- Unisys Corporation
  http://www.unisys.com
- Security First Corp.
  http://www.securityfirstcorp.com