Host based Storage Security

Sudhir Rao, IBM

Larry Hofer, Emulex

Learning Objectives

- Understand how the disruptive technologies of server virtualization and network convergence produce new security exposures that need to be addressed;
- Understand new datacenter requirements for virtualized and converged compute infrastructures;
- Understand the HbSS architecture, how it addresses new security exposures, and demonstrate dynamic virtual machine workload movement with workload-bound but portable LUN-level access controls and end-to-end data encryption;
- Understand the components of the HbSS architecture and their integration: systems management software, virtual environments, enterprise-class key management, and secure encryption HBAs; and
- Understand how to integrate security management into storage lifecycle management for secure storage provisioning.

Agenda

- New Data Center Requirements
  - Why – virtualization and convergence
  - Use case improvements
- HbSS Architecture
  - Components
  - Demo

New Data Center

New Security Requirements

Current Storage Security

Current storage security models inadequate

- Traditional SAN security advantages are lost
- Application servers rely heavily on SAN security to protect data

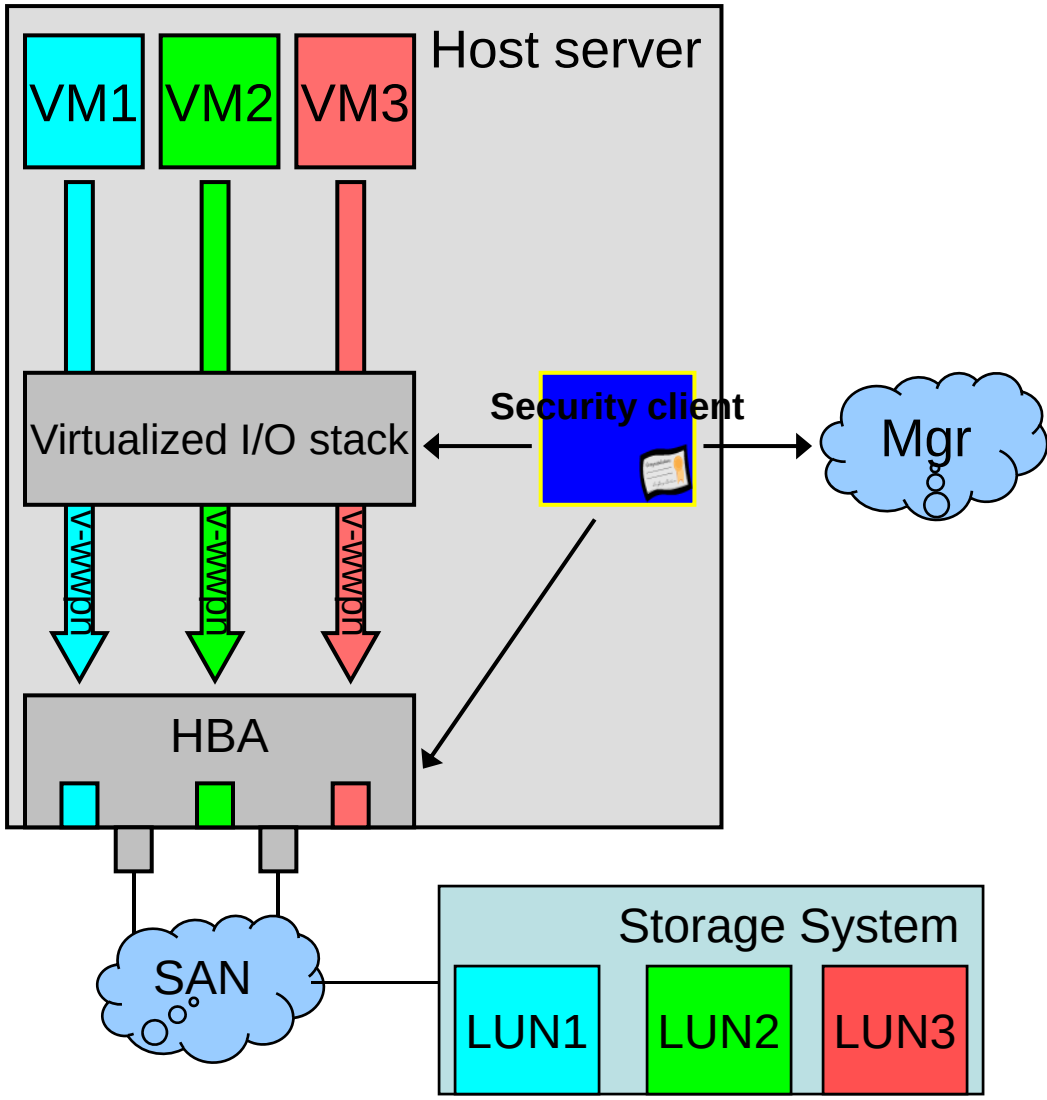
Host-based Security

New environments demand new storage security solution

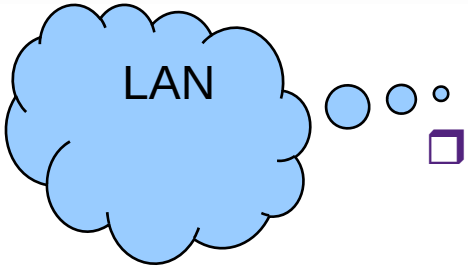
- Virtualization-aware
- Host-centric solution to storage security
- Converged Ethernet further increases need for data protection

Use Case Improvements

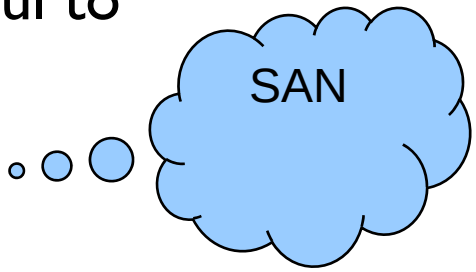
- Virtualized hosts
  - A major customer concern is lacking security solutions
- VM movement
  - No need to change SAN configuration for security
- Security end-to-end across diverse network infrastructure



Converged Networks



- Increased connectivity, creates even more security exposure
  - Makes it imperative to protect data in flight
- Today, per transport/technology solutions
- Slow adoption of standards in place long ago, even when they exist
  - Will be even worse with increased choices of transport/connectivity
- Higher layer security most helpful to encourage adoption

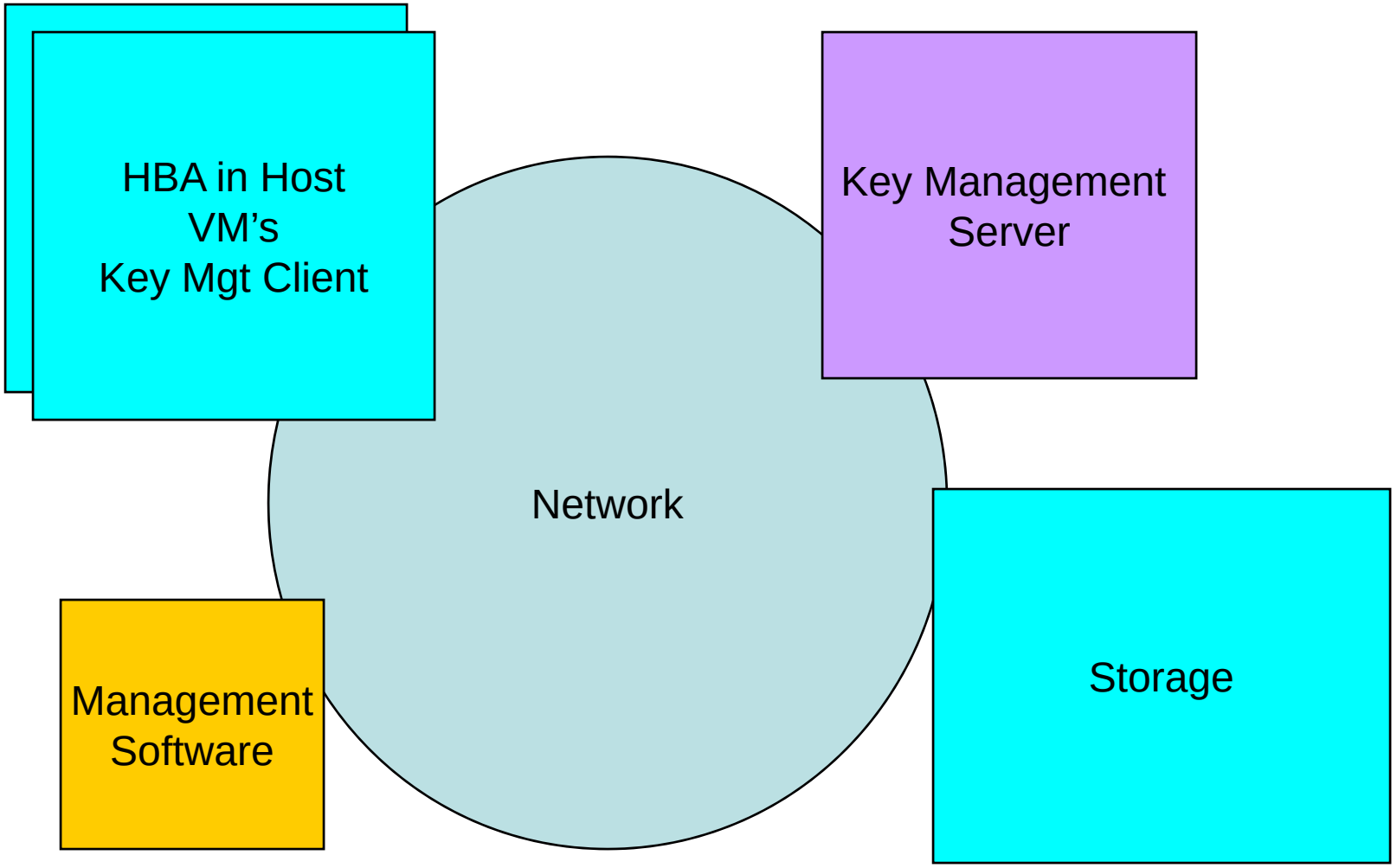


Host based Storage Security

- New approach puts the center of weight on the host to protect its data
  - Better security, less dependent on SAN components
  - Apply controls to data classification, virtualization
- The solution includes
  - Encryption in host HBA
  - Access control to LUNs
  - Centralized policy-based management: identity, access, authentication and key management

Host Based Encryption

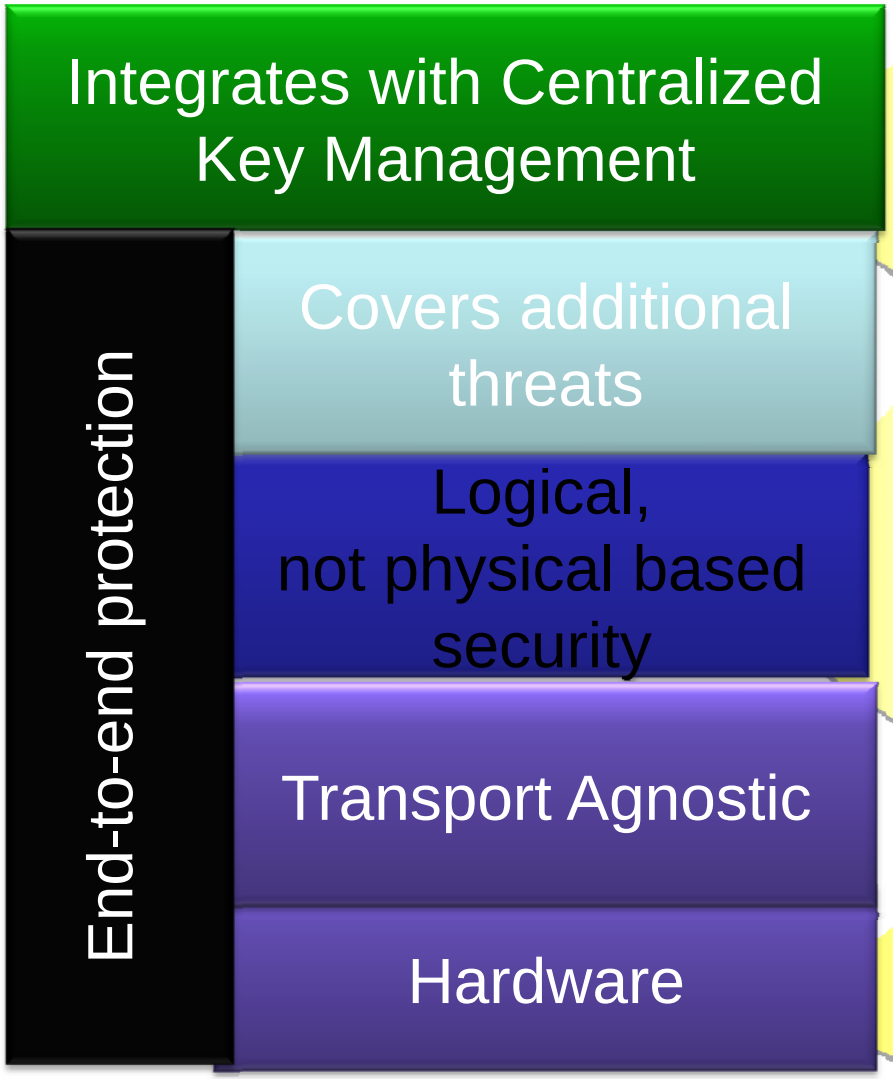
Host Based System Architecture



Host Based Encryption

Apply Security to logical volumes not physical Drives.

Data is encrypted once, protected in flight and at rest.



- Key assigned to LUN – better confinement for compromised keys
- Keys are more isolated from the encrypted storage
- Access Control Policies
- Data Classification Policy
- Mapped to Virtual Machines & applications
- Stronger Security

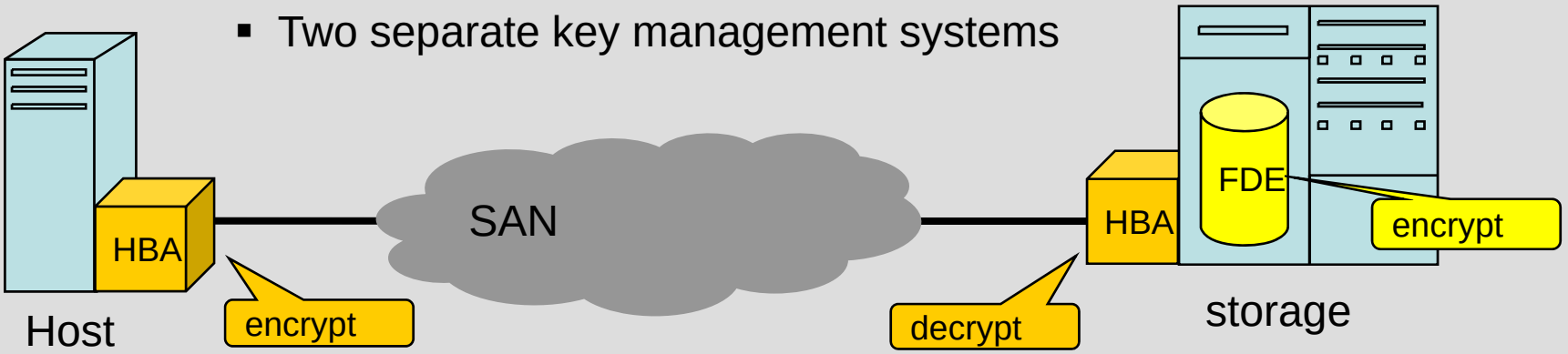
Why HBA-based security?

- Protect data as soon as it leaves the application server
  - Data is encrypted in flight and at rest.
  - Converged networks makes it imperative to encrypt data-in-flight
- Apply security to logical volumes rather than physical drives
  - Logical, mapped to virtual machines and applications
  - Access control policies
  - Data classification policies
- Access control
  - Tie access control policy to access to encryption keys
  - Apply to logical volume – map to virtual machine or application
- Hardware based solution
  - Better performance, stronger security

Encrypting data in flight and at rest

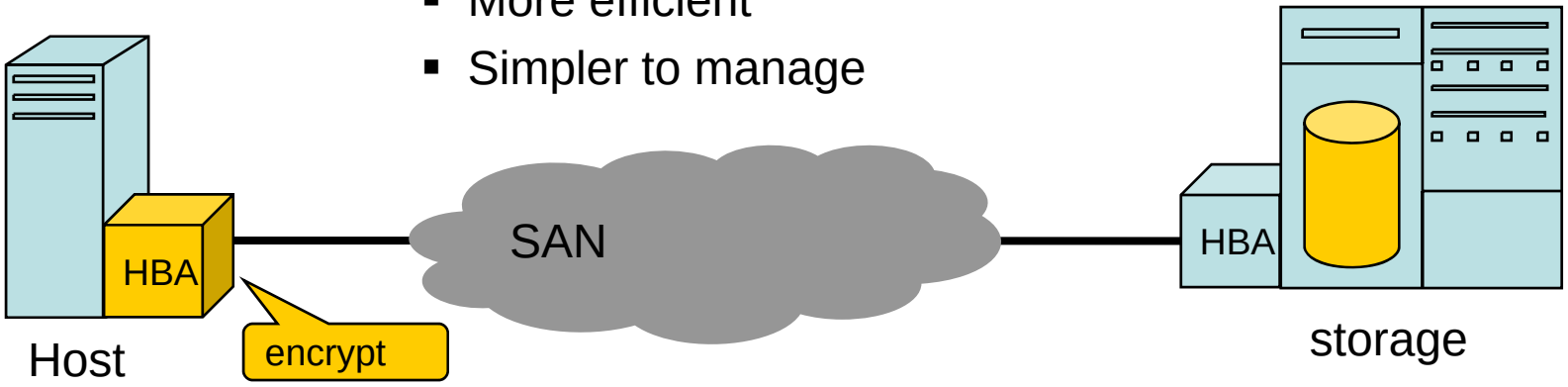
Combining network encryption with FDE encryption

- Encrypt-decrypt-encrypt
- Two separate key management systems



End-to-end HBA encryption

- More efficient
- Simpler to manage



HbSS management

1. Authentication (for systems rather than humans)
2. Authorization – Access control policy (systems access to storage volumes)
3. Cryptographic key serving and life cycle management
4. Interface component that can serve encryption keys and credentials to systems.
    1. Secure communication

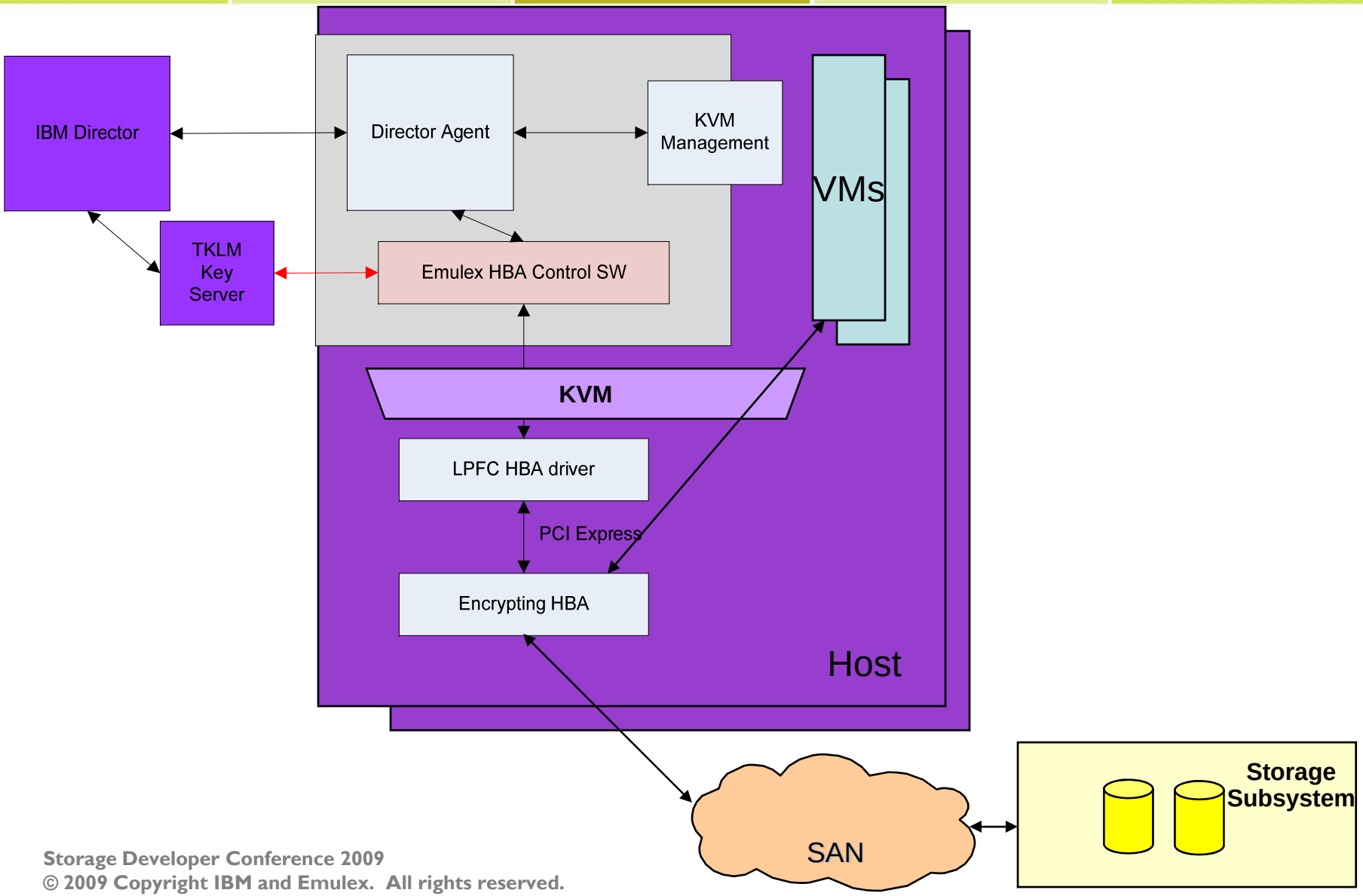
- In addition, audit log and compliance reports

Proof of Concept

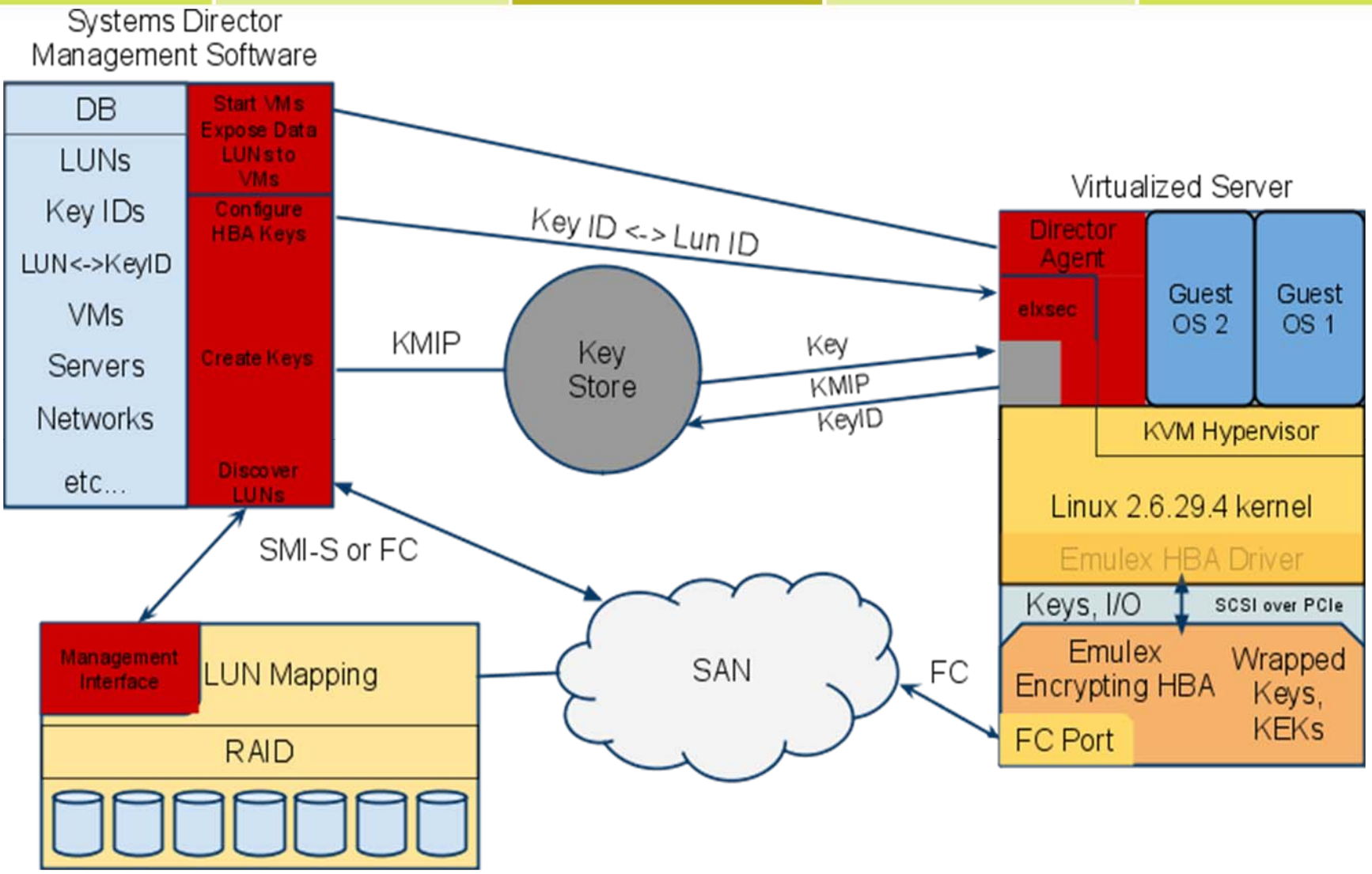
VM End-to-end data encryption

- Use Systems Director to configure its Emulex FC HBA to have the necessary security credentials to perform data encryption in-flight to pre-selected LUNs.
- Use TKLM components to manage the keys involved for encryption. The feature includes access control policy configuration and host system authentication.
- Demonstrate
  - **Integration model** between Director, TKLM, and Emulex's FC HBA
  - **Storage Discovery and Key Creation** via TKLM server
  - **VM/LUN provisioning**
  - **End-to-end data encryption**
  - **Migration of VM's**
  - **Host-centric virtualization and image management scenario** via Director for HbSS.
  - **Isolation of LUN information** on shared storage

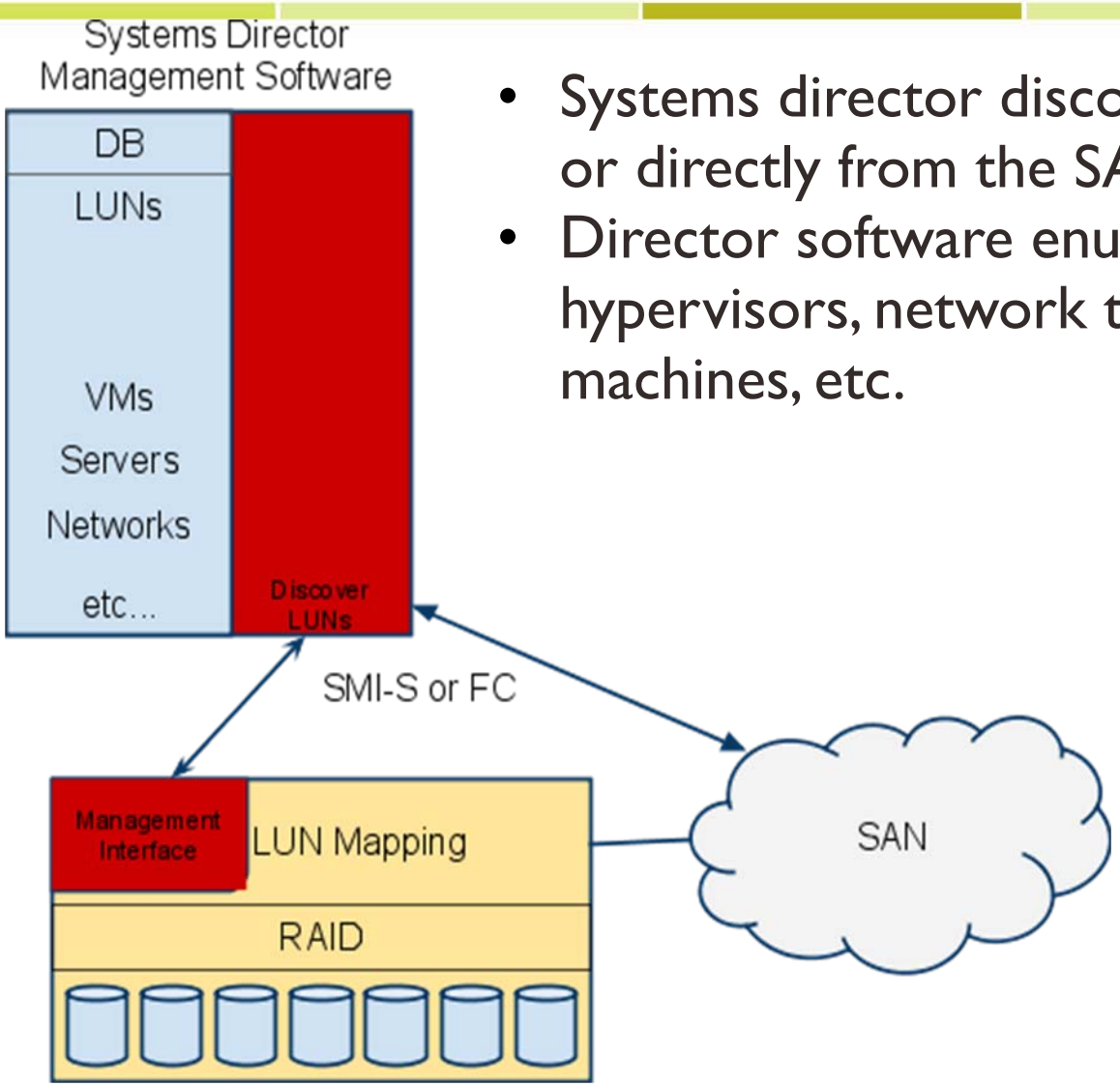
Physical Components



Overview

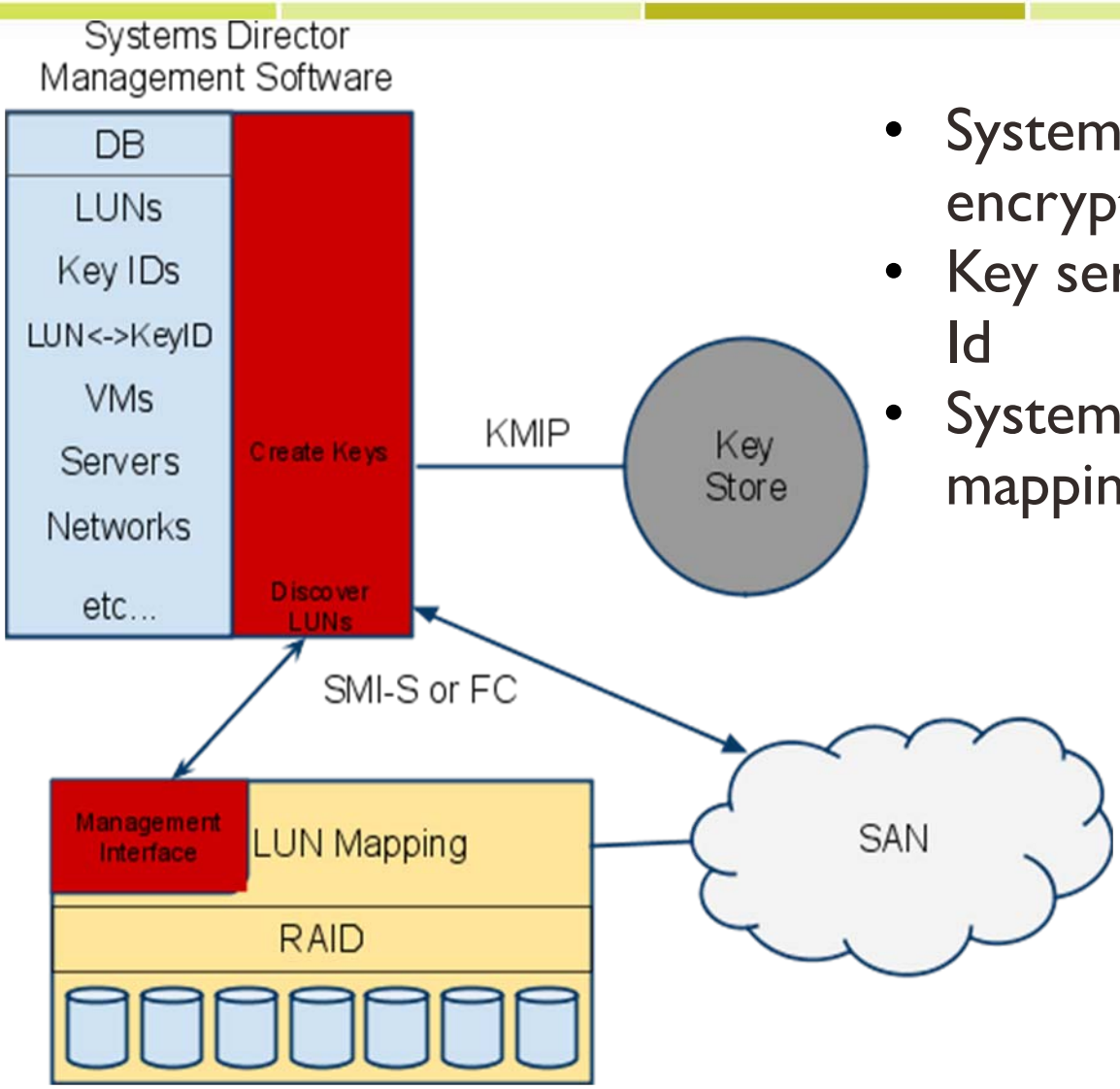


Device Discovery



- Systems director discovers LUNs via SMI-S or directly from the SAN
- Director software enumerates servers, hypervisors, network topology, virtual machines, etc.

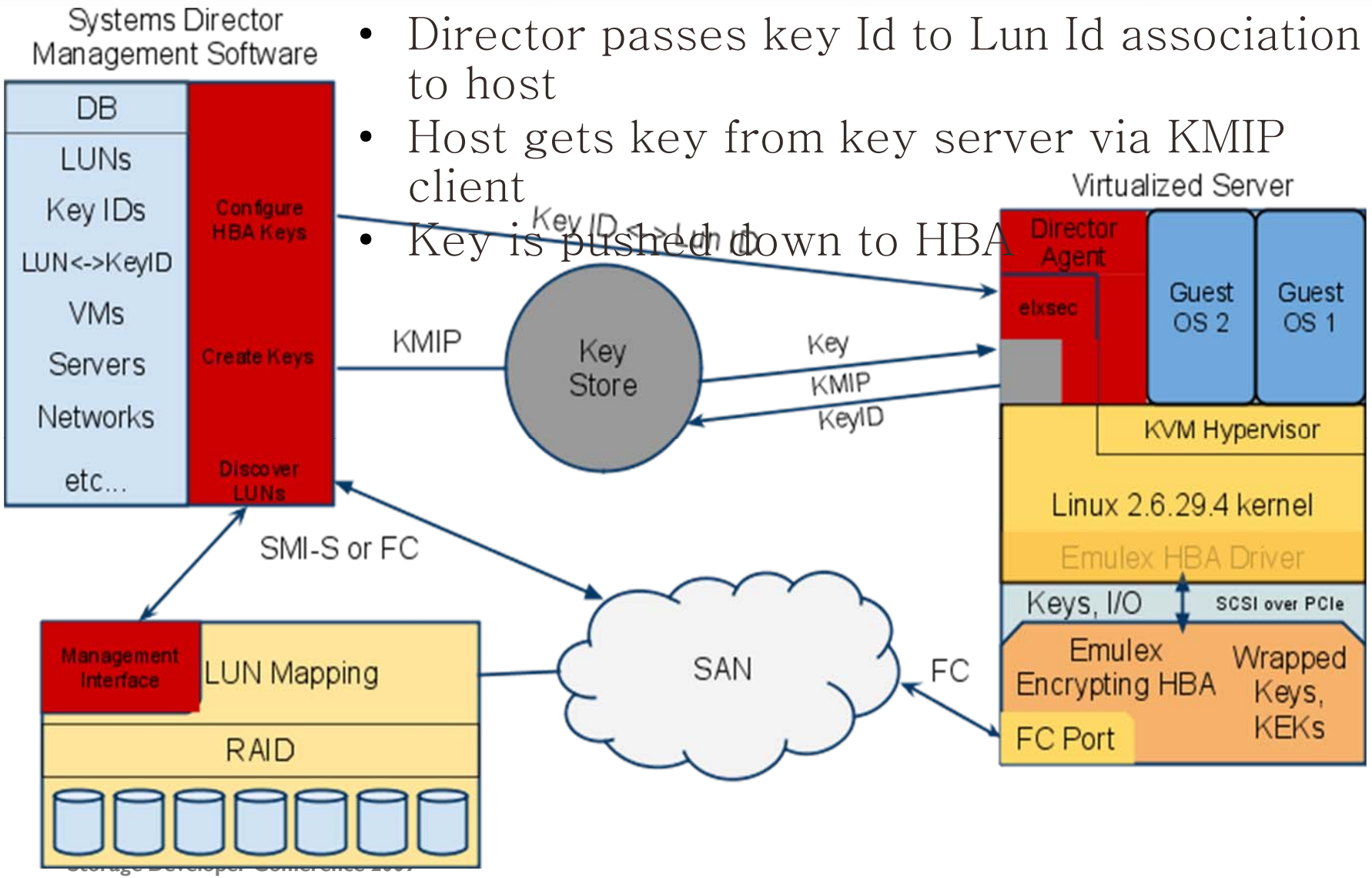
Key Creation



- Systems director generates encryption key in key store.
- Key server returns unique key Id
- Systems director persists mapping of key Id to LUN Id

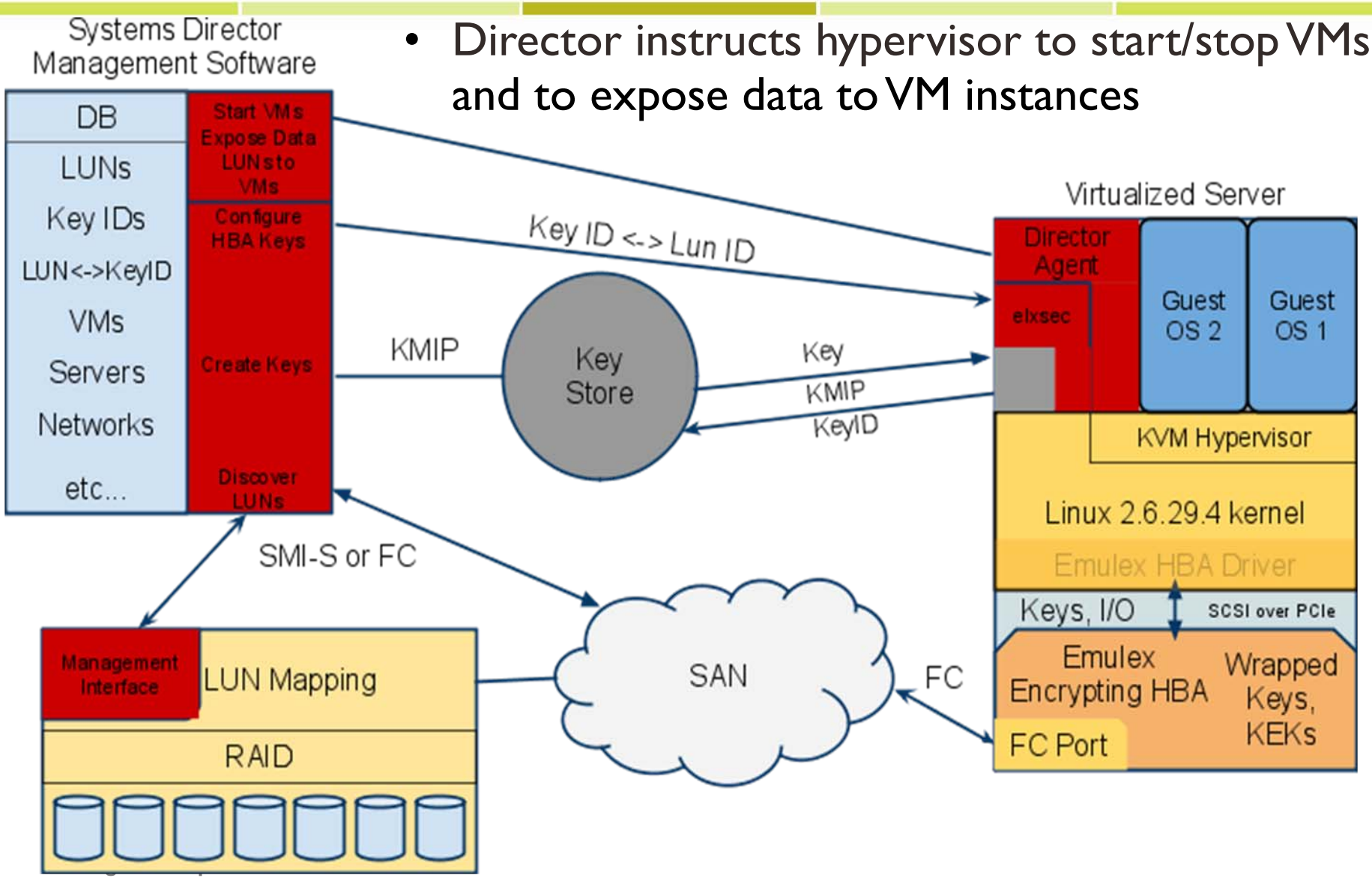
Key Provisioning

- Director passes key Id to Lun Id association to host
- Host gets key from key server via KMIP client
- Key is pushed down to HBA



Virtual Machine Management

- Director instructs hypervisor to start/stop VMs and to expose data to VM instances



Thank You!