IBM

Secure LU Access

Michael Factor, Dalit Naor, Julian Satran, Sivan Tal
IBM Haifa Research Lab, Sep 2006

Background – security and SCSI

- Environment
  - Security is a major concern in the IT industry
  - Modern SAN environments should support multi-tenancy and server virtualization in a protected and secure way.
- SCSI security in reality
  - Today initiator and target communicate over a network. Target port is shared. Logical Unit may be shared.
  - No access control or security is applied
  - Rely on underlying transport service to provide that function

Background – SAN security in reality

- Security is applied in the FC layer (for FC SAN), consisting of port zoning and LU-to-port mapping and masking.
  - Static configurations that don't fit dynamic environments
  - Protection only - not security (no port authentication)
  - Covers connection, does not cover the logical semantics of the operations performed over the connection
  - LUN masking is non-standard, vendor-specific
  - Applies to ports which may be shared among logical hosts
  - Management is complex and error prone, TCO is high
- The combination of N_Port Virtualization (NPIV) and channel security (FC-SP) resolves only part of the above issues
  - and it's expensive
  - and it's specific to FC
  - The wrong level of abstraction (managing logical entities by ports…)

Existing SPC access controls

- Section 8.3 in SPC-4
- Introduced in SPC-3.
- Affects which LUs are reported by REPORT LUNS command for a given initiator ID
- In essence – a standard for SCSI commands based LUN masking
- No authentication or any cryptographic support for spoofing prevention and integrity assurance
- No known implementations on the market

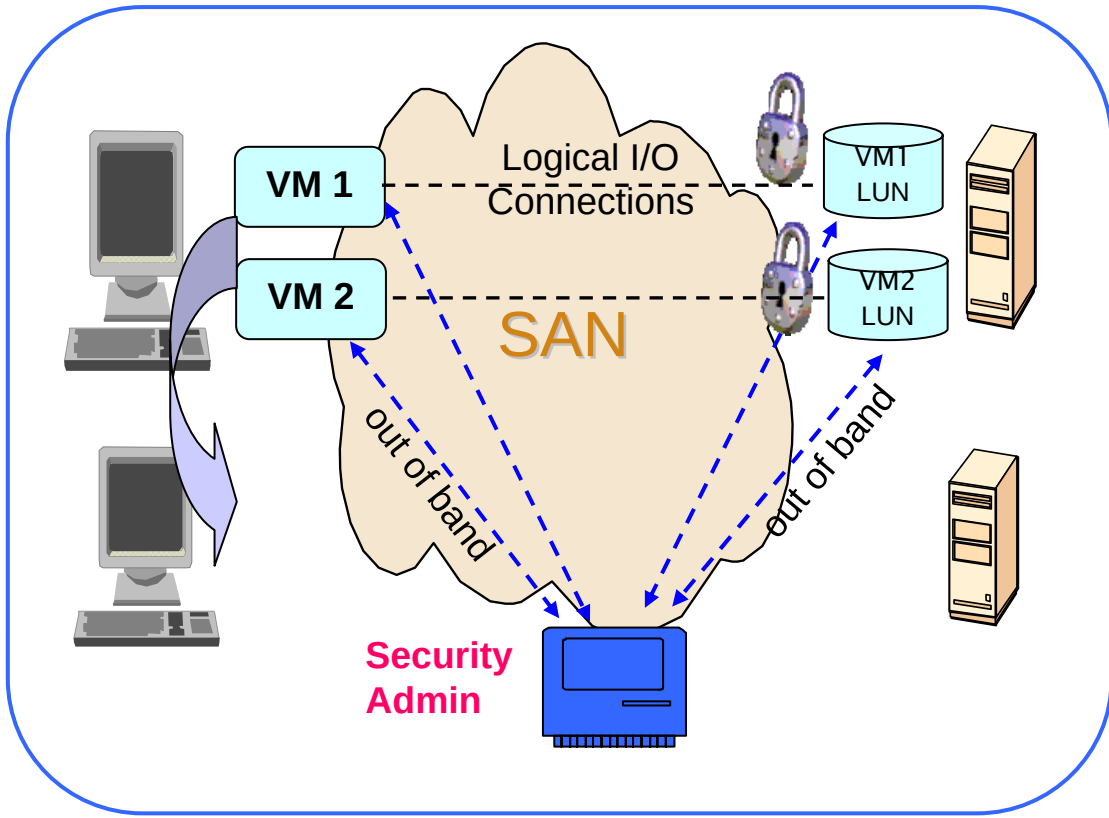
Proposed approach

- A new approach to SAN security: Apply to the logical level, implement in the SCSI protocol
  - Map Object Storage Device (OSD) security model to block devices
    - Object → Logical Unit
  - Suited for server virtualization: inherently logical rather than physical
  - Address security at command level rather than transport level – over operation rather than over connection
  - End-to-end – SCSI initiator to target, not involving FC/SAN components, independent on the SAN infrastructure.
  - Simplified management – uniform platform, one pane of glass

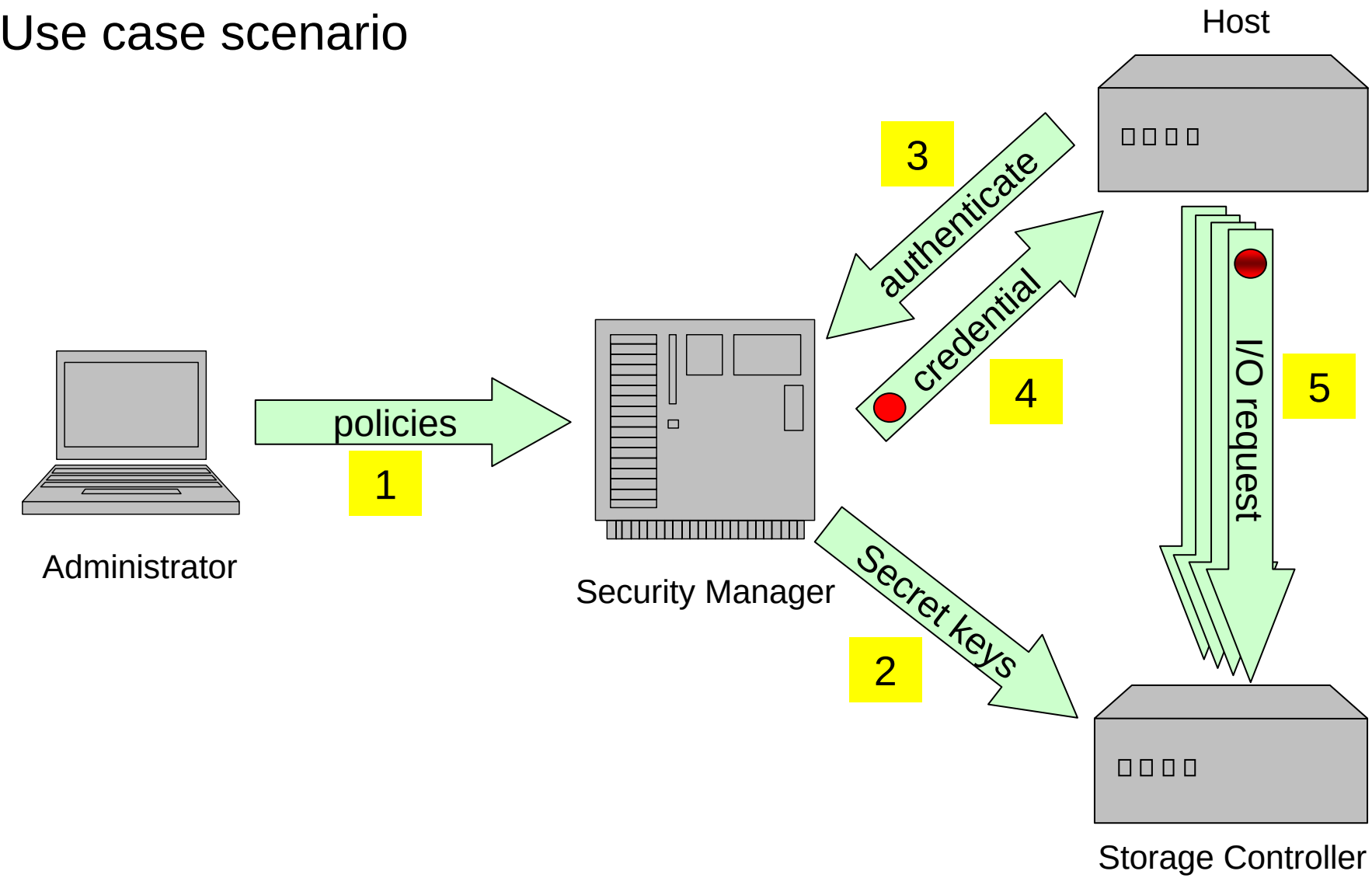
Our approach: Dynamic and secure access to LUN

- Provide a mechanism for dynamic policy enforcement
- Every access to a LUN must provide a credential, obtained from a security/policy manager
- The storage system grants/denies access based on the credential
- Credentials are cryptographic
- Purely logical, not physical
- Provides secure segregation between independent VMs
- Supports VM migration
- End-to-end, dynamic, integrated security involving servers and storage

Virtualization of Security



Use case scenario



Tentative structure of a secure command CDB

A “regular” command CDB…

… is encapsulated in a variable length CDB

Typical CDB for 16-byte commands

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE							
1	miscellaneous CDB information			SERVICE ACTION (if required)				
2	(MSB)							
3				LOGICAL BLOCK ADDRESS (if required)				
4								
5								(LSB)
6								
7				Additional CDB data (if required)				
8								
9								
10	(MSB)							
11				TRANSFER LENGTH (if required) PARAMETER LIST LENGTH (if required) ALLOCATION LENGTH (if required)				
12								
13								(LSB)
14	miscellaneous CDB information							
15	CONTROL							

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (7Fh)							
1	CONTROL							
2 - 6	Reserved							
7	ADDITIONAL CDB LENGTH (116)							
8 - 9	(MSB)			SERVICE ACTION (000Eh)				(LSB)
10 - 11	Reserved							
12 - 27	REQUEST CDB							
28 - 83	CAPABILITY							
84 - 123	SECURITY PARAMETERS							

subject to review

Additional items in the protocol: Inquiry of security parameters; key exchange