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…)
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
Use case scenario

1. **policies**
   - Administrator

2. **Secret keys**
   - Security Manager

3. **authenticate**
   - Storage Controller

4. **credential**
   - Host

5. **I/O request**
   - Storage Controller
Tentative structure of a secure command CDB

A “regular” command CDB… … is encapsulated in a variable length CDB

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