Flash Memory Summit

Security for Networked Flash Storage

“Fast Security for Fast Flash”

Bob Doud

Sr. Director of Marketing, Mellanox

bdoud@mellanox.com

Santa Clara, CA
August 2017

Rising Focus on Storage Security

- Shared data center storage means co-mingled data
  - Cloud usage models and virtualized hardware

- Threats are not just coming from the “outside”
  - Attacks are increasingly launched from **inside** the data center
- Security should be distributed, not just at perimeter
  - Ideally close to the data “owner” or source

Methods to Protect Storage

- Protect data “in-flight”
  - Encryption technologies like IPsec, TLS/SSL
- Protect data “at rest”
  - AES-XTS sector/block level encryption
  - e.g. Self-Encrypting Drives
- Authenticate user or process access to data
- Protect data against alteration
  - e.g. HMAC Hash, T10-DIF signature before encryption

Networked Flash is the New Wave

- Disaggregates storage from the compute
  - Better scaling: Need more storage?... Add another shelf
  - Better utilization
- NVMe over Fabrics
  - Negligible latency and throughput hit
  - Standardized drivers included w/ Linux
- Many OEMs rolling-out NVMe-oF products in 2017 / 18

Flash Memory Summit

New Challenges w/ Networked Storage

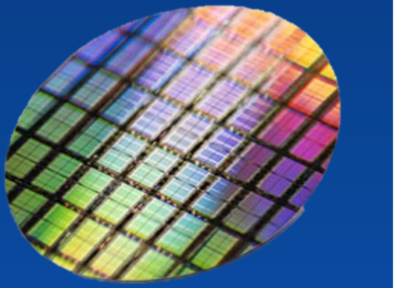
- Flash storage demands high-performance security
  - Low-latency (<5us) security processing
  - High throughputs – 100Gb/s and higher

- Key agility
  - Ability to engage many keys for encrypting / authenticating namespaces
- Protocol recognition
  - Manipulate NVMe-oF, iSCSI, etc. in order to encrypt payload

Flash Memory Summit

Silicon Solutions for Security

- New generation silicon in HBAs and Storage Controllers are able to encrypt/authenticate at wire-speed
  - Engines for AES encryption and SHA-2 hashing
- Device must understand the storage protocol AND the crypto protocol
  - Crack-open storage verbs to encrypt the payload
  - Process the crypto protocol in HW for speed and low latency



Best Practices for Security

- Implement security using standardized algorithms and protocols
  - AES, SHA2, RSA, etc.
  - IPsec, AES-XTS, etc.
- Follow Key Management standards
  - i.e. TCG OPAL
- Look for security certifications
  - FIPS-140-2

Flash Memory Summit

Thank You

Bob Doud
Sr. Director of Marketing, Mellanox
bdoud@mellanox.com

Mellanox TECHNOLOGIES