Flash Memory Summit

Hardware-Accelerated Security Offloads for Networked Storage

Bob Doud, Mellanox TECHNOLOGIES

Flash Memory Summit

Security Landscape

- Security concerns run throughout the data center
  - In the Network
    - Data theft, Access Control, Denial of Service
  - Where data is Stored
    - Theft, Alteration
- Exacerbated by:
  - Cloud adoption (shared infrastructure)
  - Higher data rates (25, 50, 100G)
  - More sophisticated threats

Flash Memory Summit

Security Toolkit

- Firewall, Access controls
- Encryption
  - Data in flight
  - Data at rest
- Secure Authentication
  - Hash-based data integrity, source validation
- Deep Packet Inspection (DPI)
  - Inspect for malware, proper connection behavior, etc.

But Security Tools Come With a Cost

- Security functions – encryption, inspection – consume significant resources at >10G speeds
- Result:
  - More CPU resource consumed
  - Lowered throughput
  - Higher Latency
- … and it's difficult to fully protect:
  - Policy settings
  - Cryptographic Keys

Hardware Co-processing Helps

- **Offload** host CPU
  - More cycles for host to run app's and virtual functions
  - More power-efficient to run on adapter
- **Accelerate** performance
  - Higher throughput (Gbps)
  - Greater packet-per-second (pps) rates
  - Lower latency
- **Secure** execution environment
  - Security functions run in isolated, embedded environment
  - Keys, credentials, policies segregated from host

Flash Memory Summit

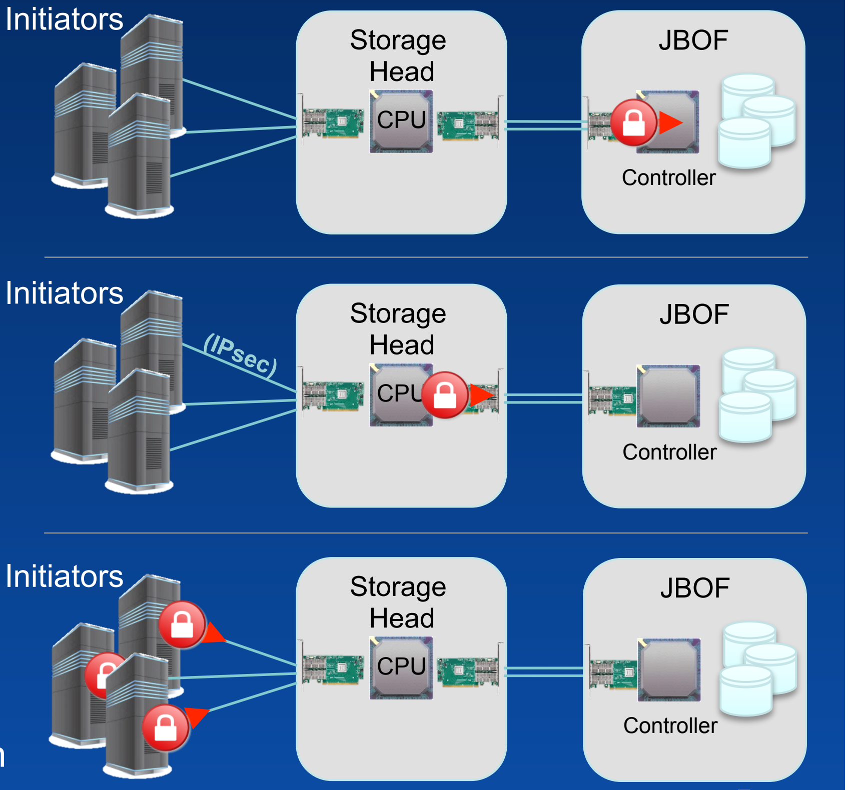
Securing Data at Rest

- Standard for disc/block encryption: IEEE P1619
    - AES-XTS encrypts without data expansion
- Provides for encryption, but no authentication
- Easy de-commissioning of drive (wipe the key)
- Protects data by requiring authenticated unlock of key(s)

- Widest deployment in Self-Encrypting Drives (SED)

Encryption Positioning

- At the Target
  - Secure data on drives
  - Simplify FIPS 140 certification
- At the Controller
  - Secure data on drives and in-flight to JBOFs
  - Centralizes security
- At the Initiator
  - Secure data over entire lifecycle
  - Owner of data controls keys



* However, target cannot compress or search

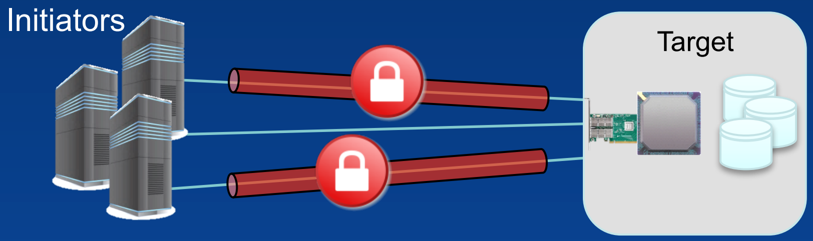
Flash Memory Summit

HW Acceleration Options

- To achieve Flash memory speeds, HW offload is needed
  - One NVMe drive demands ~25Gb/s performance
  - In Flash storage appliances, need 100Gb/s ++
- In-line vs. Lookaside acceleration
  - In-line is superior – lowest latency
  - But requires protocol awareness in the HW
- Key agility enables multi-user security

Securing Data in Flight

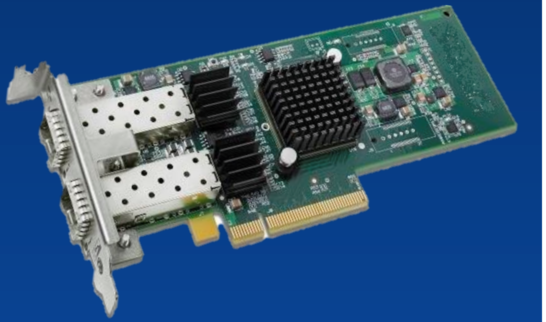
- IPsec, SSL/TLS, MACsec
  - Encryption, data integrity, source authentication
  - Protects communication between initiator and target



- Similar to “At-Rest”, acceleration needed at >10Gb/s

HW for Data in Flight Security

- Acceleration NICs are available with crypto offload
  - Single PCIe slot for I/O & security
  - Incorporate policy engine + crypto + packet header/trailer processing



- Advanced products protect the crypto keys on-board the NIC
- SmartNICs can accelerate the secure handshake as well

Flash Memory Summit

Accelerating Policy / ACLs

- Firewall functionality can be an important security tool
  - Control access to storage resources
  - Microsegmentation is the latest buzz around fine-grained policy

- Advanced NICs & SmartNIC's incorporate wire speed parse-classify engines
  - Match-Action policies – e.g. drop, forward to host/VM
  - SDN control plane to configure tables

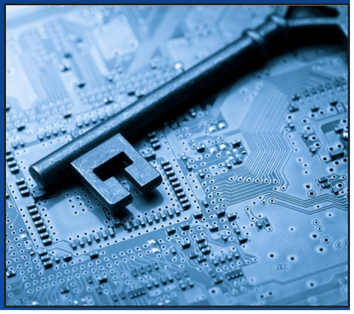
- SmartNICs can isolate the control plane

Flash Memory Summit

Distributed Security

- Security should be deployed where sensitive data is stored and processed
  - Protecting data over the network or at rest
  - Protecting the datacenter infrastructure from attacks
    - both from outside and from inside

- SmartNICs dramatically improve security posture
  - Secure boot / trusted firmware
  - Hardened OS and security app’s
  - Protected & isolated policy and key management

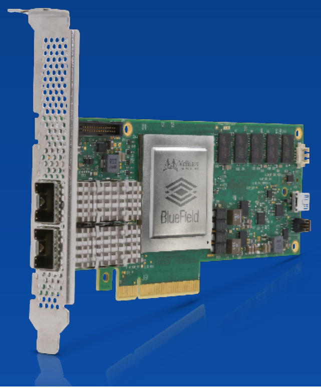


Summary

- Storage Security is a hot topic
  - Protect data with: Encryption

    Authentication

    Access-control policy
- Hardware is available to accelerate these functions
  - Preserve host CPU cycles
  - Maximize IOPS and throughput
  - Minimize any latency adder



Thank You

Bob Doud

bdoud@Mellanox.com