SNIA

STORAGE NETWORKING INDUSTRY ASSOCIATION

EDUCATION

Alternative Approaches to Storage Security

Michael Fahey, Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individuals may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced without modification
  - The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.

Abstract

Alternative Approaches To Storage Security

This session will focus on encryption for data at rest with several storage architectures and explain various alternatives for key management. There are many legal, regulatory, and security requirements that may conflict with one another. For example, certain compliance requirements may not be met with common key management practices. Simplified key management using the encrypted storage medium itself may offer the privacy protection that is required and meet other legal and regulatory requirements at much lower cost.

What Are You Worried About?

- Is it security?
- Or is it compliance?
- You need to establish what the goals are that you are trying to achieve and what the threat is that you are trying to protect against

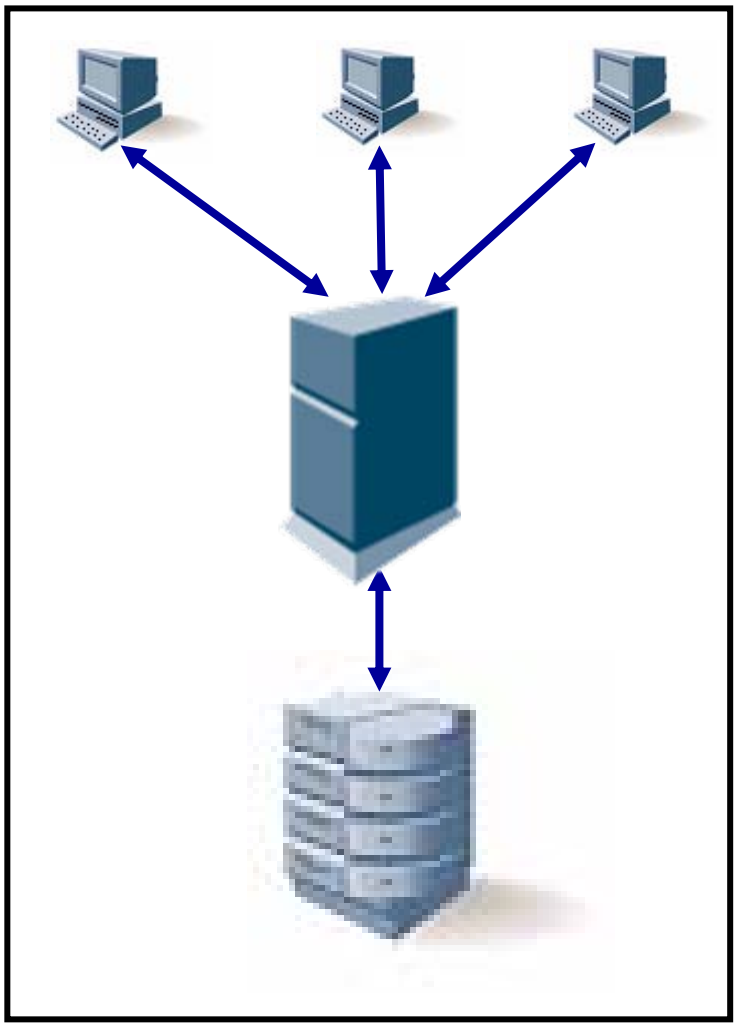
Agenda

- Physical security
- Authentication
- Other Processes
  - Drive security
- Introducing Encryption
  - Storage Key Management
- Archiving and Key Management
  - The Security Dichotomy
  - SEC 17a4
- Another approach
  - Secret sharing

Options

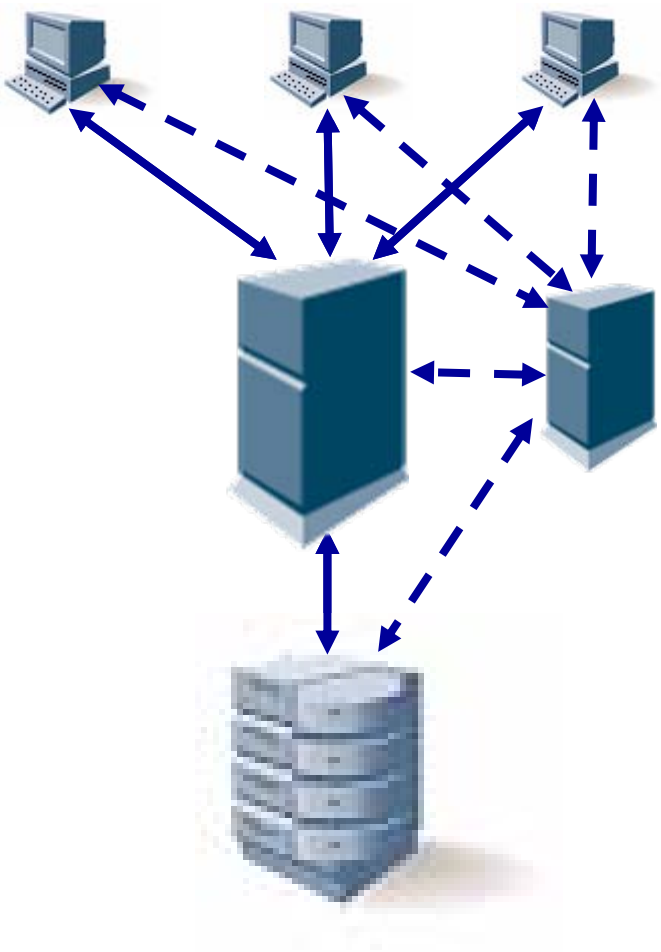
- There are several options for preventing unauthorized access to confidential information
- If ‘just enough security’ is enough, then choices exist outside of certified encryption solutions
  - Some will not be encryption based
  - Some will be encryption based
- Is privacy protection the goal?

Total Physical Security



- End-users, application servers, and storage are physically isolated from the rest of the world
- End-users are assumed to be trusted parties
- Nothing else can get in or get out
- Great in concept, hard to implement in practice

Authentication



- End-users are authenticated against a trusted platform
  - Application server and storage are still isolated from the rest of the enterprise
- And/or application server is authenticated against a trusted platform
  - Storage is isolated from the rest of the enterprise

Other Processes

- What happens if someone leaves the data center with a disk drive?
  - Total physical security would never let someone in or out with disk drive
  - But what if you don't have total physical security?
- All drives removed from storage are destroyed
- Or all drives removed from storage are electronically wiped (DOD 5220.22-M)
  - Implemented as a service or done in house
- All of the above have human dependencies!

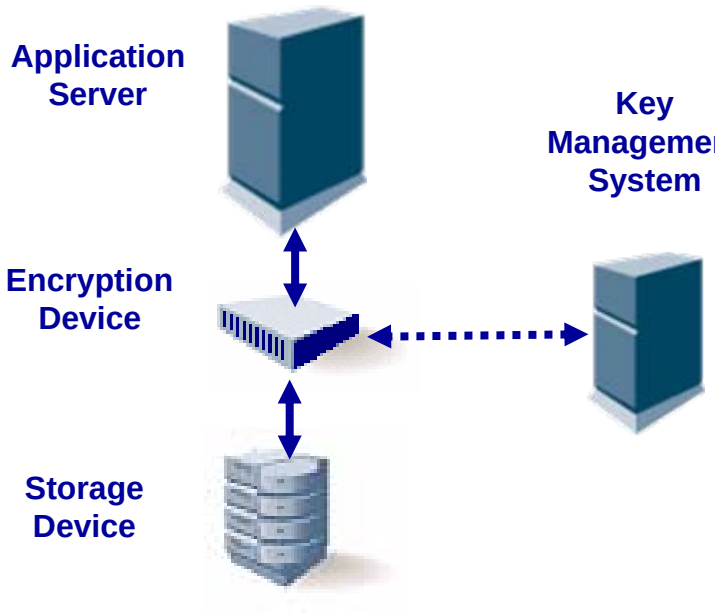
Disk Drive Security

- As an alternative or in addition to physical security encryption at rest is an option
- Disk drives removed from storage don’t need to be destroyed or erased as they are already unreadable
- Less human dependence
- More automated process
- Does not address authentication!

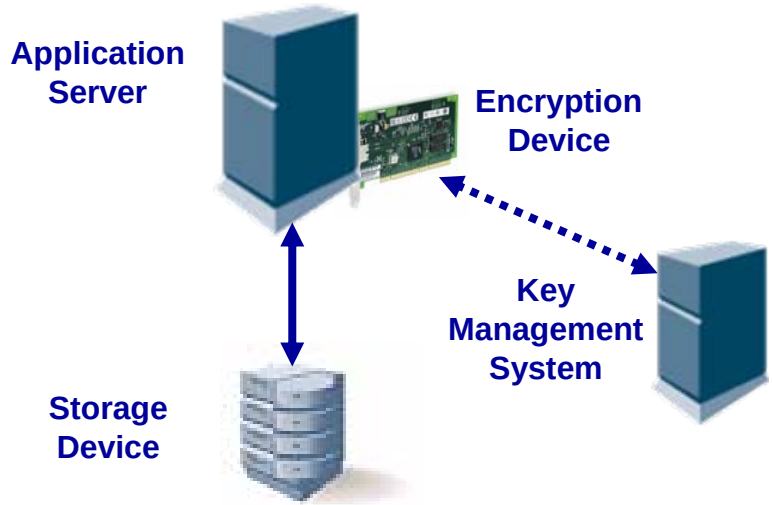
What is Encryption and Storage Key Management?

- A storage device (LUN or file system volume) has all content within it encrypted by an encryption system as information is written to it and decrypted by it as it is read.
- An encryption key is used to write and must be used to read information
- The key is stored on an a Key Management System
  - Some encryption systems use in band appliances
  - Others use on-board components working with the application server

External Key Management



In-Band Appliance



On Server

Another Regulation

- SEC 17a-4 is the only US regulation that requires WORM storage
- SEC 17a-4 is the ‘gold standard’ which many companies use for governance even without a compliance requirement
- SEC 17a-4 requires that all functionality for WORM and accessibility be intrinsic to the storage medium
- How do I do that with an external key management system?
- Many SEC 17a-4 compliant storage systems do not use encryption today

Archiving and Security

- In a long term archive, how do I ensure that the key encrypting my archive will always be there and available for reads and writes from the archive medium?
- Systems and storage will change over the life of the archive
- The key allowing access to my archive is not in the archive
  - It is not intrinsic to the storage medium

Another Approach

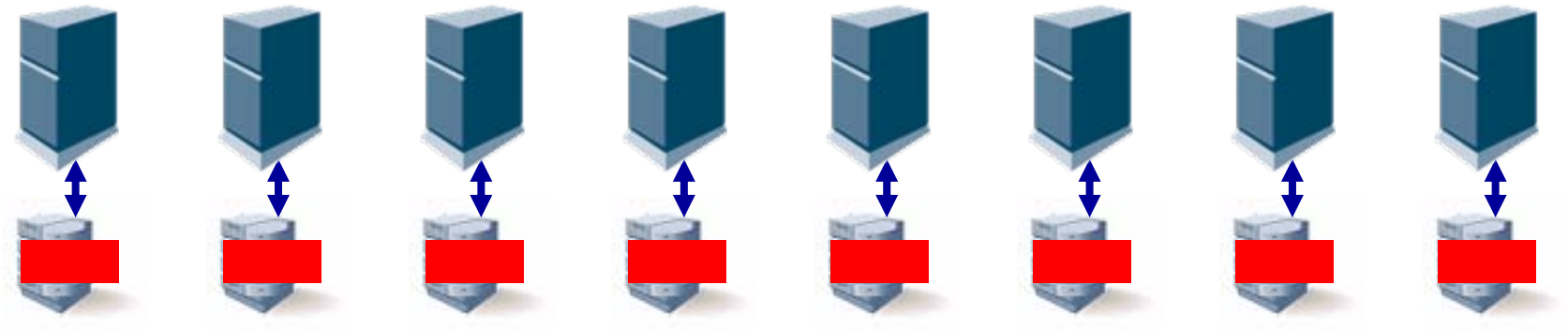
- What if the encryption key was stored within the storage medium itself?
- How do I do that securely?
- Secret Sharing
  - A key is transformed into n shares over a storage system of n devices
  - A quorum of any m devices is needed to recreate the key
  - If any individual device or subset of devices less than m is taken then nothing can be read
- This approach is not FIPS 140-2 certified

Secret Sharing in a Cluster

Key

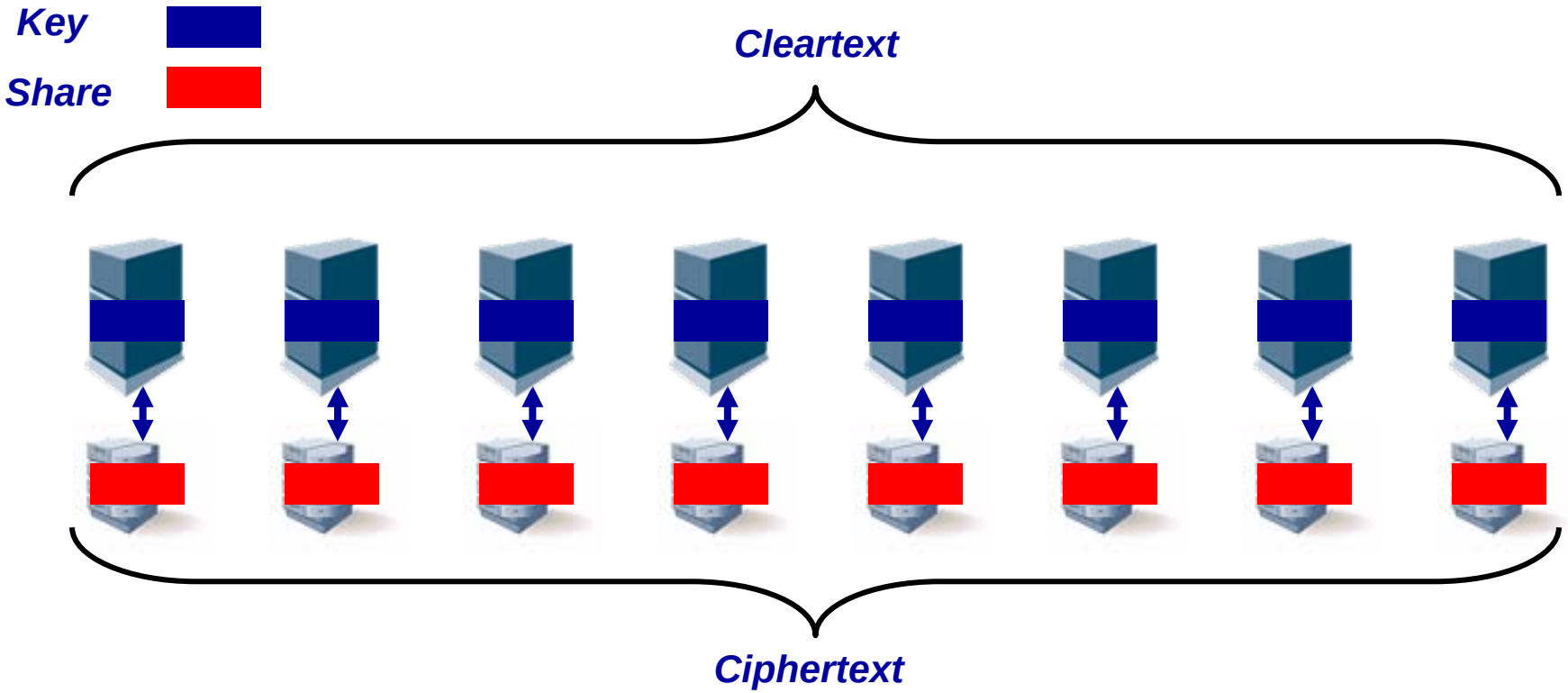
Share

In this example 8 nodes are in a cluster n=8
A quorum of 5 is chosen m=5



The key is transformed into 8 shares with one stored on each node in the cluster

Secret Sharing in a Cluster



Upon powering up the cluster with at least 5 nodes the key is recreated and stored on each node. All content written will be encrypted and all content read will be decrypted.

Best Practices with Secret Sharing and Encryption

- The key transformation (share) results stored on each device are the same bit length as the original key
- Collecting some devices less than the quorum specified will not make it any easier to calculate the key
- Key should probably be escrowed elsewhere
- Any content that can be read after being decrypted is validated (typically 128 bits at a time) but in an archive it is probably a good idea to get a guarantee of authenticity of the file against a hash as well.

Where is Secret Sharing?

- Secret Sharing has largely been out of the mainstream
  - Self-built storage clusters in research and academia
  - Utilized in some other security products to establish a quorum (BOD, defense applications)
  - GNU GPL ssss code by B. Poettering written in 2006
- Secret Sharing could be incorporated as feature in storage products
  - Imagine a storage controller utilizing secret sharing among disk drives
  - Storage clusters can incorporate secret sharing very easily

Pro's and Con's

SNIA
Storage Networking Industry Association
EDUCATION

No Encryption

- Requires physical security
- Drives should be destroyed or erased to DOD 5220.22M
- Human dependencies
- Good for long term retention

External Key Mgt

- Many products available
- Meets FIPS 140-2
- Solves the walking disk drive problem
- Challenges for long-term retention

Secret Sharing

- You can build it yourself (or maybe your vendor will)
- Can use a wide variety of algorithms
- Will not impact SEC 17a-4
- Solves the walking disk drive problem
- Good for long-term retention

Recap

- What are your security requirements?
- Which specifically are driven by governance to internally imposed standards or compliance to external regulations?
  - This is important to resolving conflicts
- Do you have
  - Authentication?
  - An isolated network?
  - An isolated storage system?
- How do you handle a walking disk drive?
  - SLA's?
  - Encryption?

References

- Handbook of Applied Cryptography, Menezes, Oorshot, and Vanstone
- http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- http://en.wikipedia.org/wiki/FIPS_140
- http://www.sec.gov/rules/interp/34-47806.htm
- http://point-at-infinity.org/ssss/
- http://www.cacr.math.uwaterloo.ca/~dstinson/ssbib.html

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

SNIA Education Committee

Michael Fahey
Rob Mason
Eric Hibbard
LeRoy Budnik
Andres Rodriguez
Rich Rogers
David Shaw