Encrypted Storage

James Hughes

Senior Fellow

Storage Technology Corporation

IEEE-CS/SSSC/SISWG Chair

Agenda

What is *Security*
iSCSI and IPsec
Application and File encryption
Tape Encryption
Disk Encryption
File System
Interoperable Standards
What to do?

What to do?

Determine your security boundaries

- Who/what do you trust

Does Storage Encryption help

- Provides Separation

Key Management

- That meets your business model

What is *Security*

What is *Security*

A feeling

What would you tell your CEO if his laptop were stolen?
Have you destroyed all the data on those scrapped disks?
Has anyone read and/or modified your backup tapes?
Your operators are caught surfing the health records?
What do you sat to managers that refuse consolidation?

F.U.D.

Data Can be Recovered

In practice

- deleted, partial buffers
- combination of Raid and mirrors

In labs

- Spin Stands
- Atomic Force Microscope

In Theory

- Edges, Reading under

How long is your data important to your adversaries?

- What techniques will happen in the future?

What can Storage Security *Do*?

Enable storage consolidation
Coke and Pepsi sharing a

- Storage Network,
- Disk array,
- Tape library
- File server
- Archive

with their most sensitive data
Protection for data *in transit and at rest*

- End to end protection

Definitions

Privacy
Confidentiality
Authentication
Digital Signature
Integrity
Non-Repudiations
Time-stamp
Key

Key Management

Single largest issue

Network Key management

- Ethereal
- Lose one, make a new one

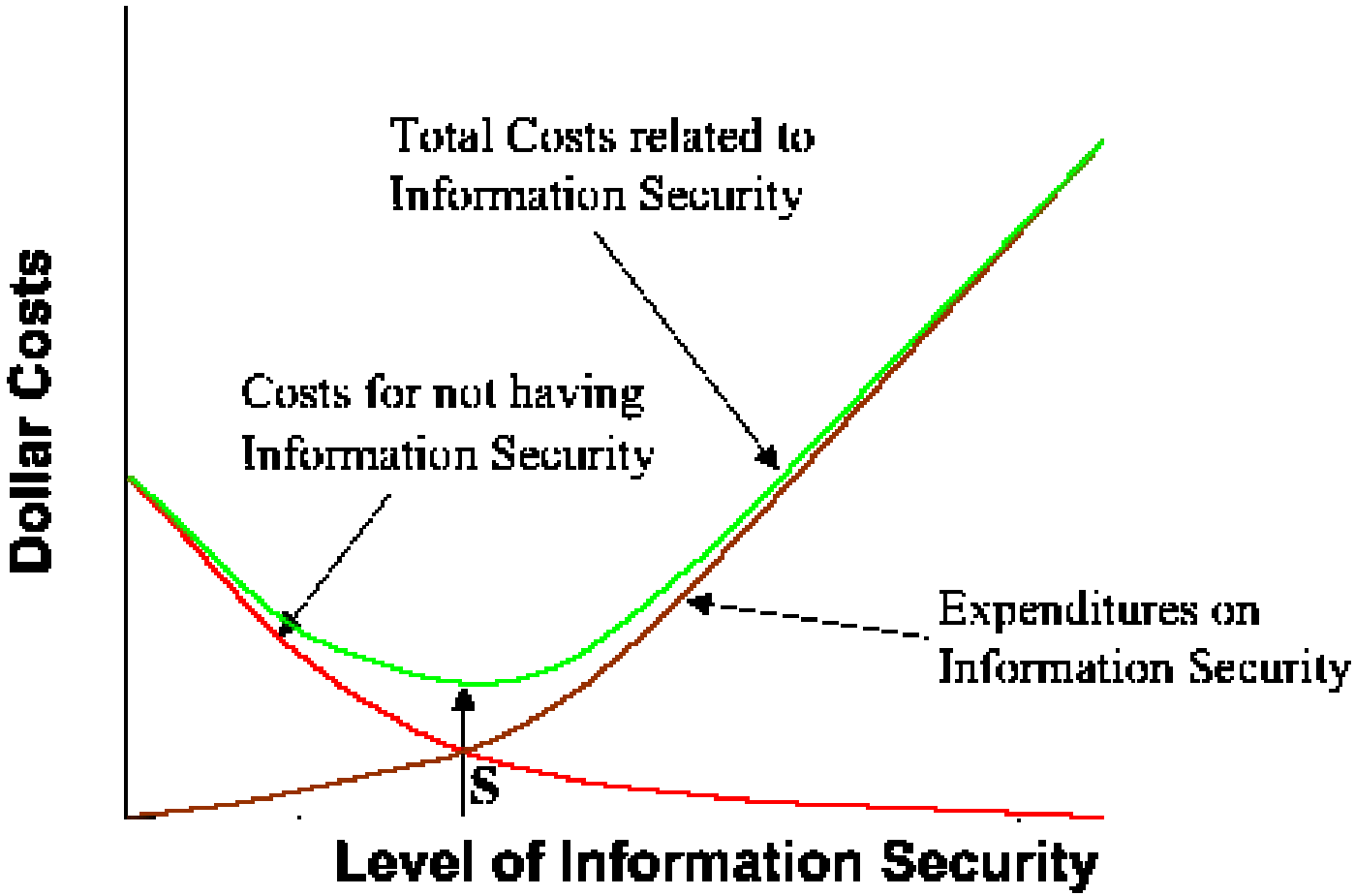
Storage is different

- Lose Keys, Lose data
- Must be prepared

Is PKI the answer?

- What is the question?

Economic Aspects



L. Gordon, R. Smith, Economic Aspects of Information Security, Tech Trend Notes, NSA, Vol. 110, No. 4, Fall 2001

iSCSI and IPSEC

iSCSI and IPSEC

Protection of data in transit

- Not at rest

Requires two encryptors

- At each end of the link

Storage Encryption only requires one

Other link encryption possibilities

FC over IP Encryption
FC over SONET encryption
FC over ATM encryption

Remainder focused on confidentiality of

- data in transit and at rest

Application and File encryption

StorageTek

Application and File encryption

PGP

- Web of trust
- Individuals

Word

- Password to open

No standard

Not a general storage solution

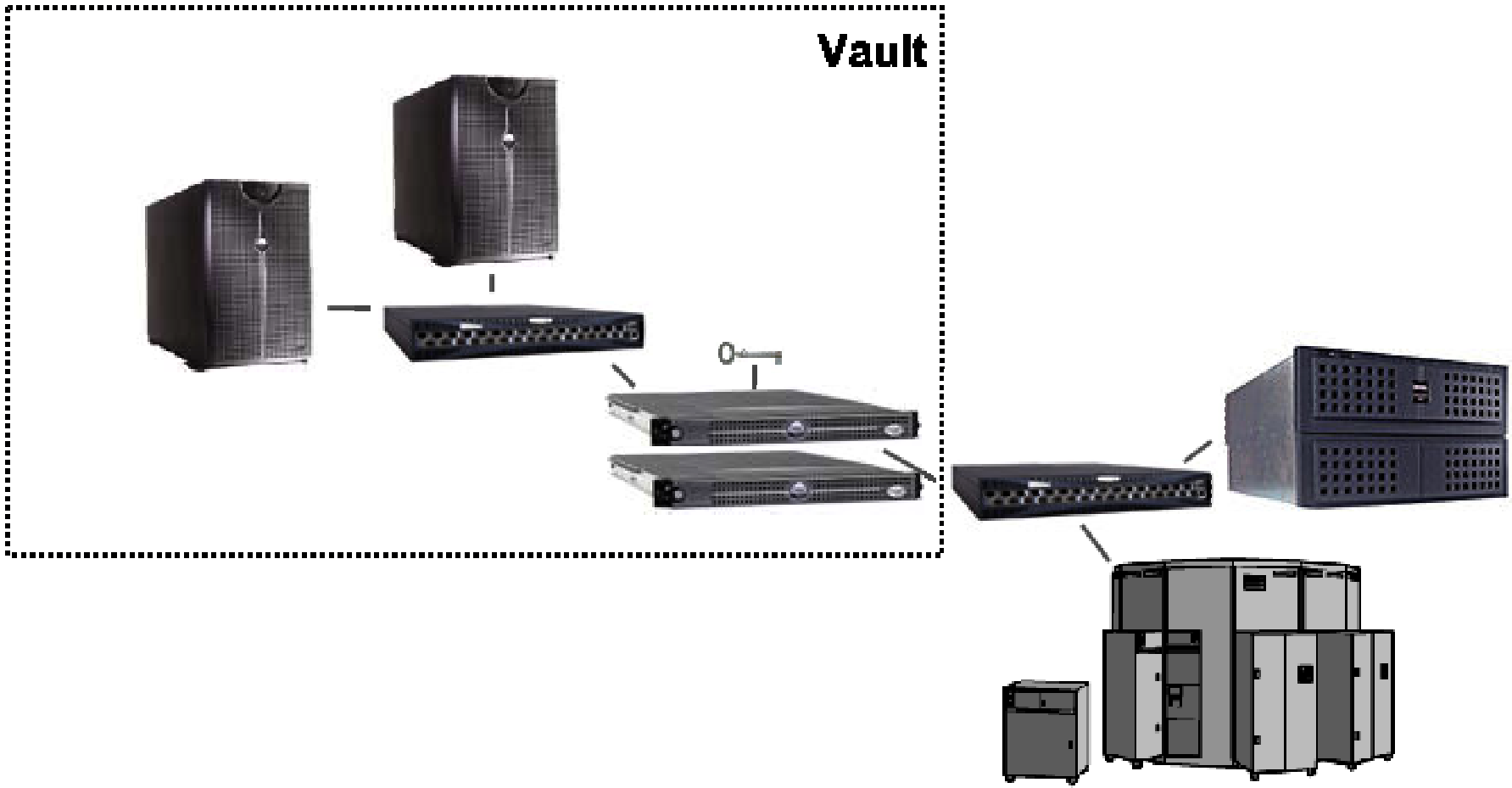
Many residual vulnerabilities

Many residual vulnerabilities

Temporary files
Page storage
Communication of passwords and/or keys
Absence of enforced perimeter
Playing Hide and Seek with the keys

- Microsoft TCB
  - The-technology-formerly-known-as-Paladium

Enforced Perimiter



Tape Encryption

StorageTek

Tape Encryption

Not New

- Then - Paranoia, Veritas,
- Now - Neoscale and others

Why Bother, Tape is dead, right?

- SneakerNet

Major issues

- Confidentiality
- Key Management
- Integrity
- Compression

Confidentiality

The information is Encrypted
Ownership if the key allows access
Can be accomplished in drivers or standalone devices

- Bump in the wire

Key Management

One key should not be used forever

- What if it is compromised
  - All is lost?

Key Management should match your business process

- Expire keys when expire data?

Integrity

Combines

- Integrity
- Digital Time-Stamp
- Signature

Allows tapes to be created, copied, migrated, moved
With the ability to prove the data has not been tampered

Virtual WORM

Compression

Encrypted data is not compressible
Current tape technology relies on compression for capacity
If encryption is performed, compression must be moved before the encryption

- Without compression encryption will lose 50% to 75%

Disk Encryption

Disk Encryption

Not New

- Then - Loopback Driver, Apple Disk Copy, PGP disk
- Now - Decru, Neoscale, Vormetric and others

Issues

- Benefits
- Modes
- Residual Vulnerability

Benefits

Disk and SAN can be protected

- Single Device

Keys can (should) be managed by users

Disks can be scrapped, sold or re-purposed

- Without vulnerability

No need to trust zoning and LUN masking

- No need to trust the administration of this

Modes

Current products use Cipher Block Chaining

- Vulnerable to block reordering

IEEE Security In Storage Workgroup

- Standardizing a replacement

Residual Vulnerabilities

Key Generation

Key Management

- Key Escrow
- Key revocation

Traffic Analysis

- Be able to determine the directory and file structure
  - (not names)

Backups through the servers

- Needs separate protection

File System

File System

Not New

- Then - CFS, stackFS, SecureFS and others
- Now - Decru, and others

Issues

- Access Control
- File Names
- Residual Vulnerabilities

Access Control

File encryption *can* augment ACLs

- Fine grain access control independent of file system
- Less need to trust file system
- Revocation of users?

Allow reading (snooping) of anything

- Use Cryptography as a separator

File Names

File names in the clear

- Allows files to be backed up while being encrypted
- Directory structure
- File names important?

Encrypted File Names

- Dictionary Attack?

Residual Vulnerabilities

File names and traffic analysis
Revoked users
Revoked Keys

Interoperable Standards

StorageTek

Algorithms

Beware of Snake-oil

Only use well known Algorithms

- AES, IDEA, Triple DES
- Single DES is obsolete and insecure

Modes are important

- CBC has problems

Standards are in process

- Modes
- Key Exchange between vendors

Interoperable Standards

IEEE-CS, SSSC, Security in Storage Workgroup

Algorithms and modes

- Significant public analysis

Key Migration Standard

- Be able to replace a vendor with another
- Without re-encrypting data

What to do?

What to do?

Determine your security boundaries

- Who/what do you trust

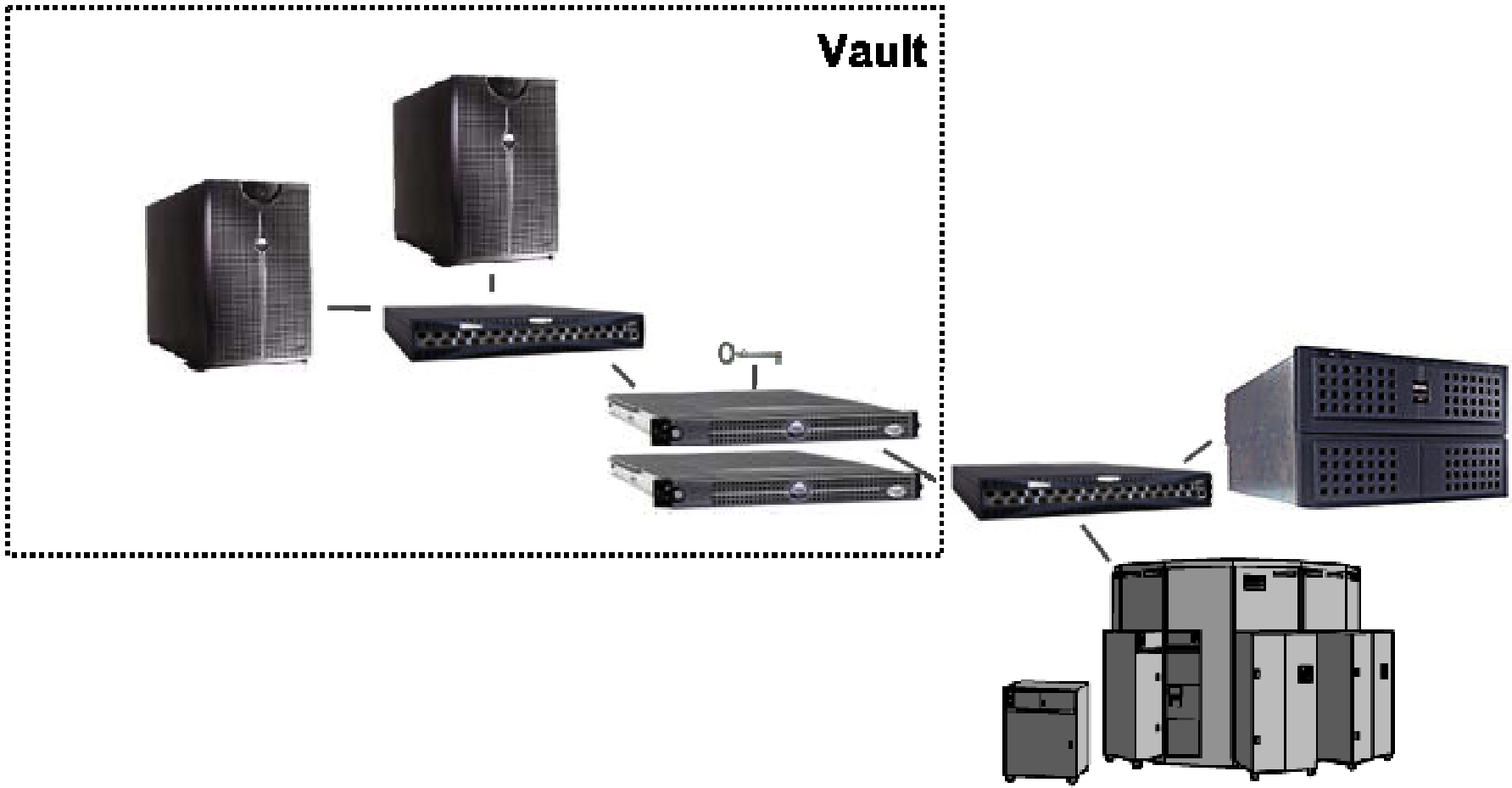
Does Storage Encryption help

- Provides Separation

Key Management

- That meets your business model

Enforced Perimiter



Questions?