Storage Encryption

Jim Hughes

Storage Technology, 7600 Boone Ave No

Minneapolis MN 55428-1002

Phone: +1-763-424-1676, Fax: +1-763-424-1776

E-mail: james_hughes@storagetek.com

Presented at the THIC Meeting at the STK Bldg 8 Auditorium, 1 Storage Tek Dr, Louisville CO 80027-9451

July 22 - 23, 2003

Encrypted Storage

James Hughes
Senior Fellow
Storage Technology Corporation
IEEE-CS/SSSC/SISWG Chair

Agenda

What is *Security*

iSCSI and IPsec

Tape Encryption

Disk Encryption

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?

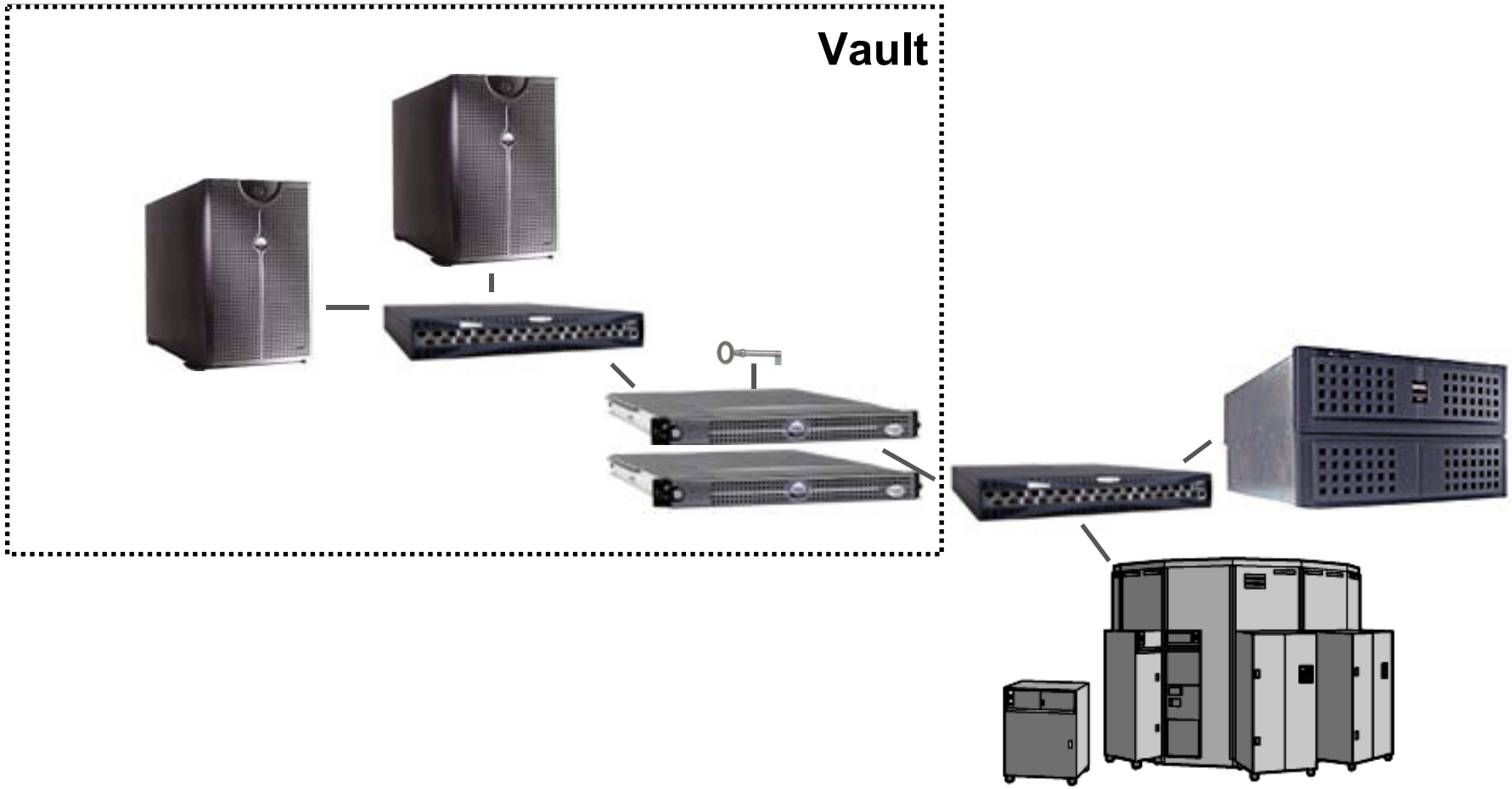
- What techniques will happen in the future?

Peter Gutmann

9. Conclusion

[...] it is effectively impossible to sanitise storage locations by simple overwriting them, no matter how many overwrite passes are made or what data patterns are written [...]

Enforced Perimiter



What can Storage Security *Do*?

Enable storage consolidation

Coke and Pepsi sharing a

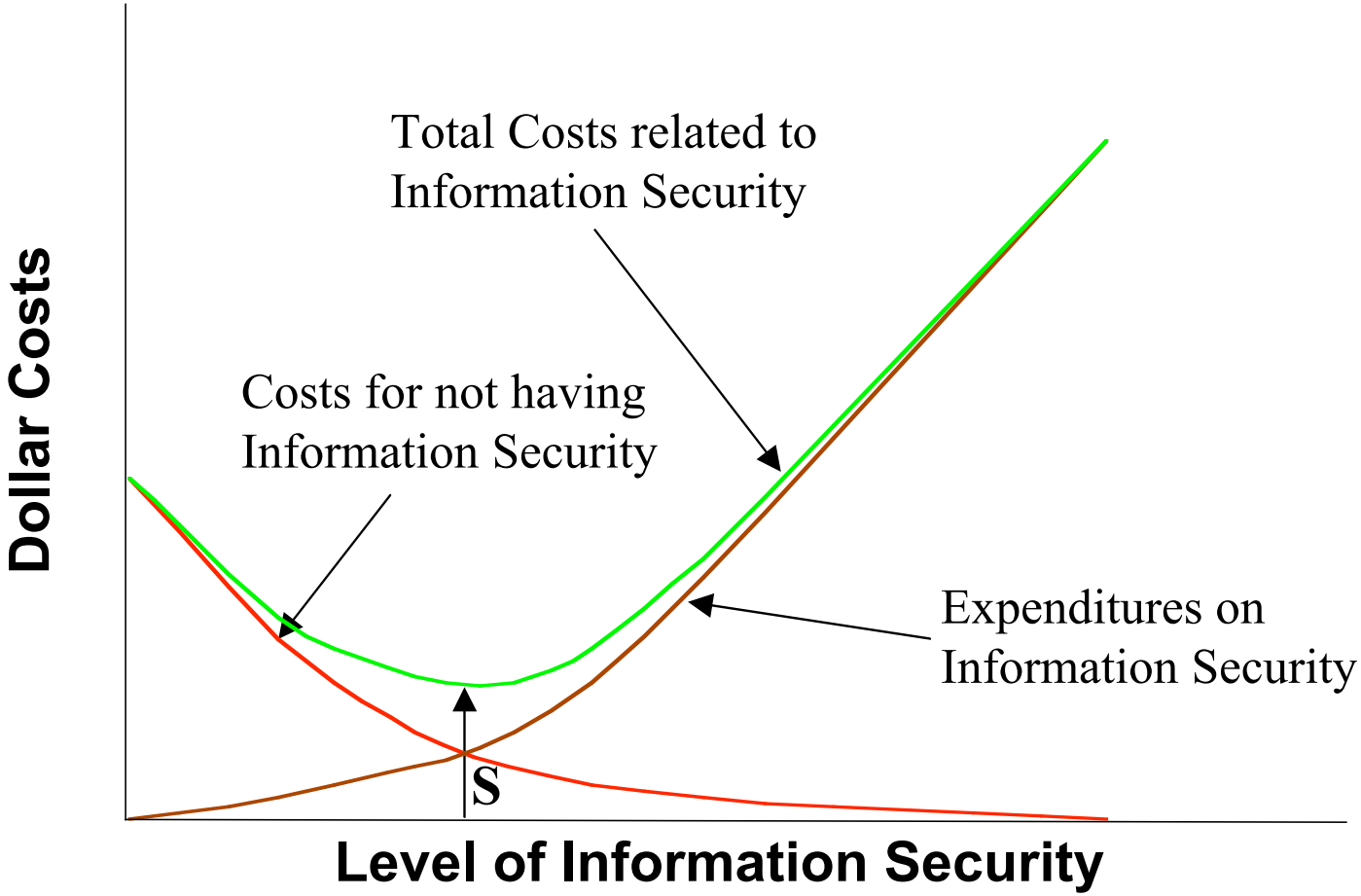
- Storage Network,
- Disk array,
- Tape library
- File server
- Archive

with their most sensitive data

Protection for data *in transit and at rest*

- End to end protection

Economic Aspects



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

Definitions

Privacy

Confidentiality

Authentication

Digital Signature

Integrity

Non-Repudiation

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?

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

Tape Encryption

Tape Encryption

Not New

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

Why Bother, Tape is dead, right?

- SneakerNet
- Bandwidth becoming MORE expensive

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 -
  - SAN: Decru, Neoscale, Vormetric and others
  - ATA/IDE: HDD

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

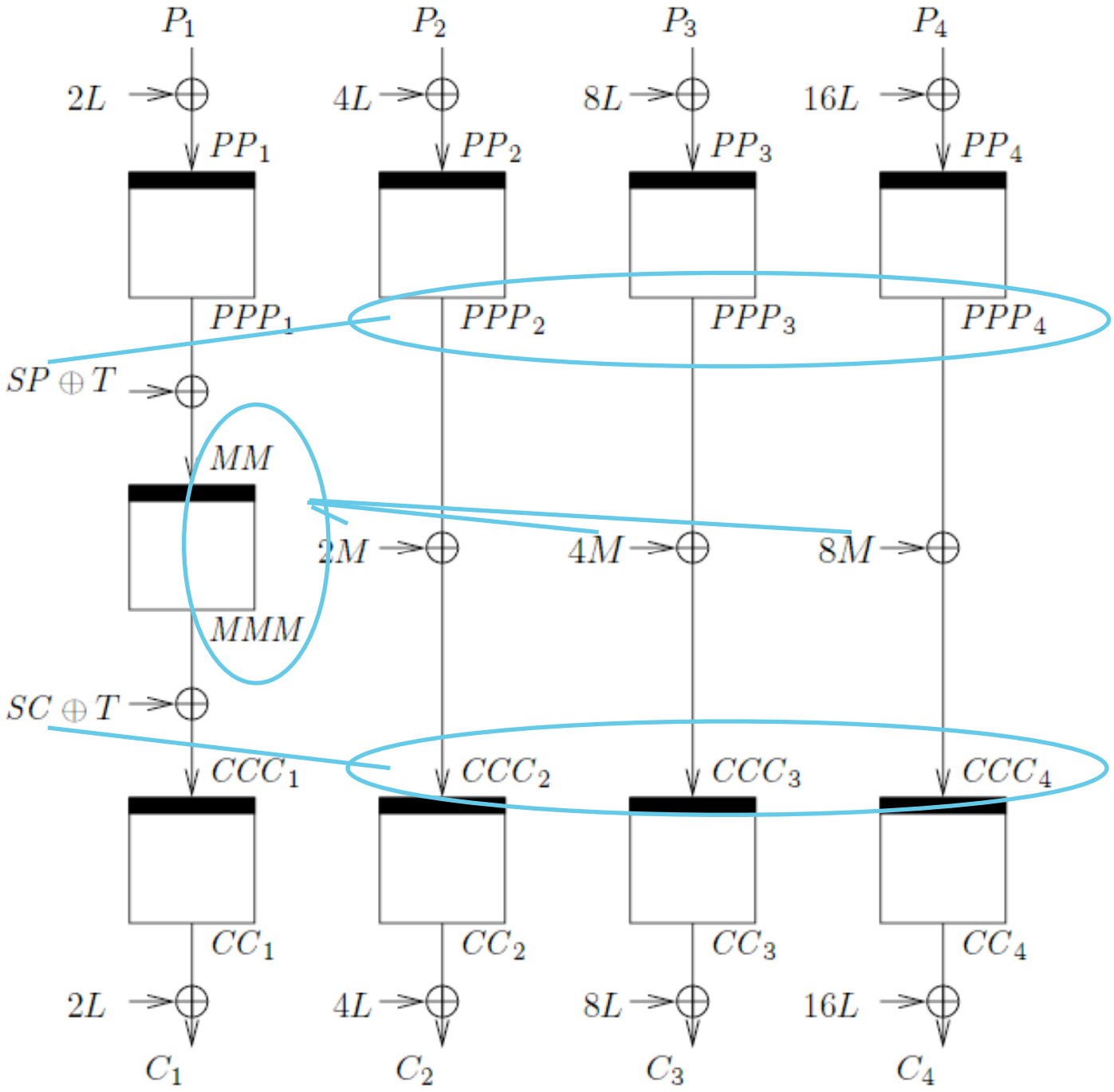
Current products use Cipher Block Chaining

- Vulnerable to block reordering
  - Within a block
  - Between Sector Location

IEEE Security In Storage Workgroup

- Standardizing a replacement

EME


P_1
P_2
P_3
P_4
$2L$
$4L$
$8L$
$16L$
PP_1
PP_2
PP_3
PP_4
PPP_1
PPP_2
PPP_3
PPP_4
$SP \oplus T$
MM
$2M$
$4M$
$8M$
MMM
$SC \oplus T$
CCC_1
CCC_2
CCC_3
CCC_4
CC_1
CC_2
CC_3
CC_4
$2L$
$4L$
$8L$
$16L$
C_1
C_2
C_3
C_4

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

Interoperable Standards

Algorithms

Beware of Snake-oil

Only use well known Algorithms

- AES, IDEA, Triple DES
- Single DES is obsolete and insecure
- RSA 1024 “Under Attack”

Modes are important

- CBC has REAL problems for storage

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?

Determine your security boundaries

- Who/what do you trust

Does Storage Encryption help

- Provides Separation

Key Management

- That meets your business model

Enforced Perimiter