



Storage Encryption

James Hughes

Sun Fellow

Solaris Chief Technologist

LSEC Security Symposium

January 22, 2009

Brussels, Belgium

Agenda

Why are we here?

What is “Storage Security”

A sampling of issues

No clear answer

What to do?

Encrypt your data

Your OS vendor must help

Why Are We Here?

CNN Moments

Laptops in amusement parks

Laptops at airports and borders

Disks bought as scrap

RAID disks stolen

LANL Thumb drive

Tapes lost in an armored vehicle

Changing the auditable for the unauditable

5-9s of offsite archive reliability

Tapes lost inside the datacenter

Terminology

Storage

Data

Information

Knowledge

Terminology

Storage

Data

Information

Knowledge

Wisdom

Nirvana

Why now?

California law on data disclosure

CEO to jail (never enforced?)

Companies fined for data disclosure

Blue Cross violated state insurance regulations

The tension of privacy and commerce

When in doubt, don't keep it

Data loss will always be here

Accidents

Crimes

Conflict Between

Data Protection

from lose (backup)

Date Protection

from disclosure

Which would you choose?

Either or Both?

Backup/Archive

using independent keys

Segregate Private Information?

Doesn't scale

Not possible?

Storage Encryption

Changes a large secret

All of your data on your site

Into a small secret

Key

If data falls into the wrong hands

“The First Secret” separates authorized from
attacker

Why are we here?

Fear Uncertainty Doubt

A failed marketing strategy

How much is enough?

Laws

Regulation

Standards

Competition

How does one choose door locks?

The situation is complicated

What is the status?

Tactical improvements

It is not possible to process encrypted data

BAND-AID® strategy

First secret problem

Need for enterprise key management

100k keys in the clear

Rogue employee

Strategic improvements

Will take time

What we know about the past

Raid is not an information security measure

8+1, 1/9 of the data is in the clear on each drive

Not spread by byte, 4k at a time

Hacking, Viruses are known problems

Disk wiping is a human intensive process

Potential for mistakes; Broken drives?

Encryption Appliances?

DRM is an impossible dream?

Insiders are and continue to be a threat

“Prediction is very difficult,
especially about the future.”

Niels Bohr

What we know about the Future

Cryptography built into the hardware

Sun Niagara, Intel Westmere*

Algorithms being improved

IEEE P1619 family

Storage encryption built into the OS

BitLocker, Encrypted ZFS

Identity Management Maturing

Key management is still ad hoc

Forensics will get harder

*According to Wikipedia

To Be Continued...

