



# 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)

Data 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...





# Storage Encryption (2)

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

# Agenda

---

“Storage Security”?

Storage contains personal information

Storage Security vs Network Security

Security Attributes of Secure Storage

Existing Systems and Sample Attacks

Performance vs Trends in Computers

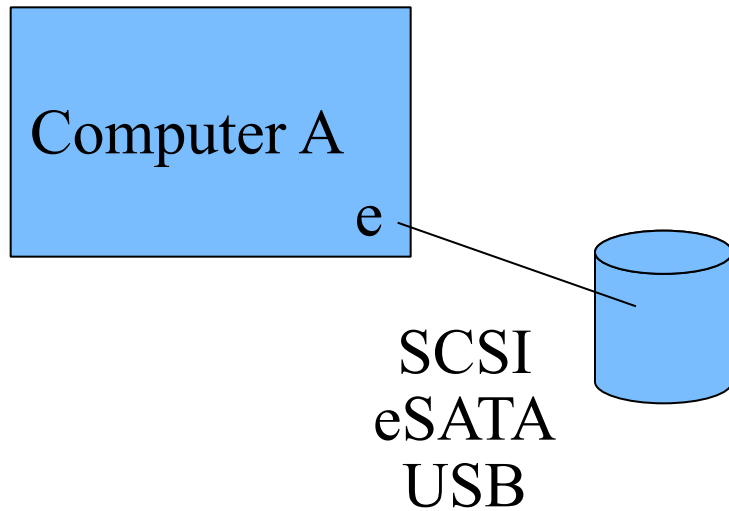
Long Term Prediction of Adoption

Areas for Future Research

# Storage Configurations

---

## Local disk

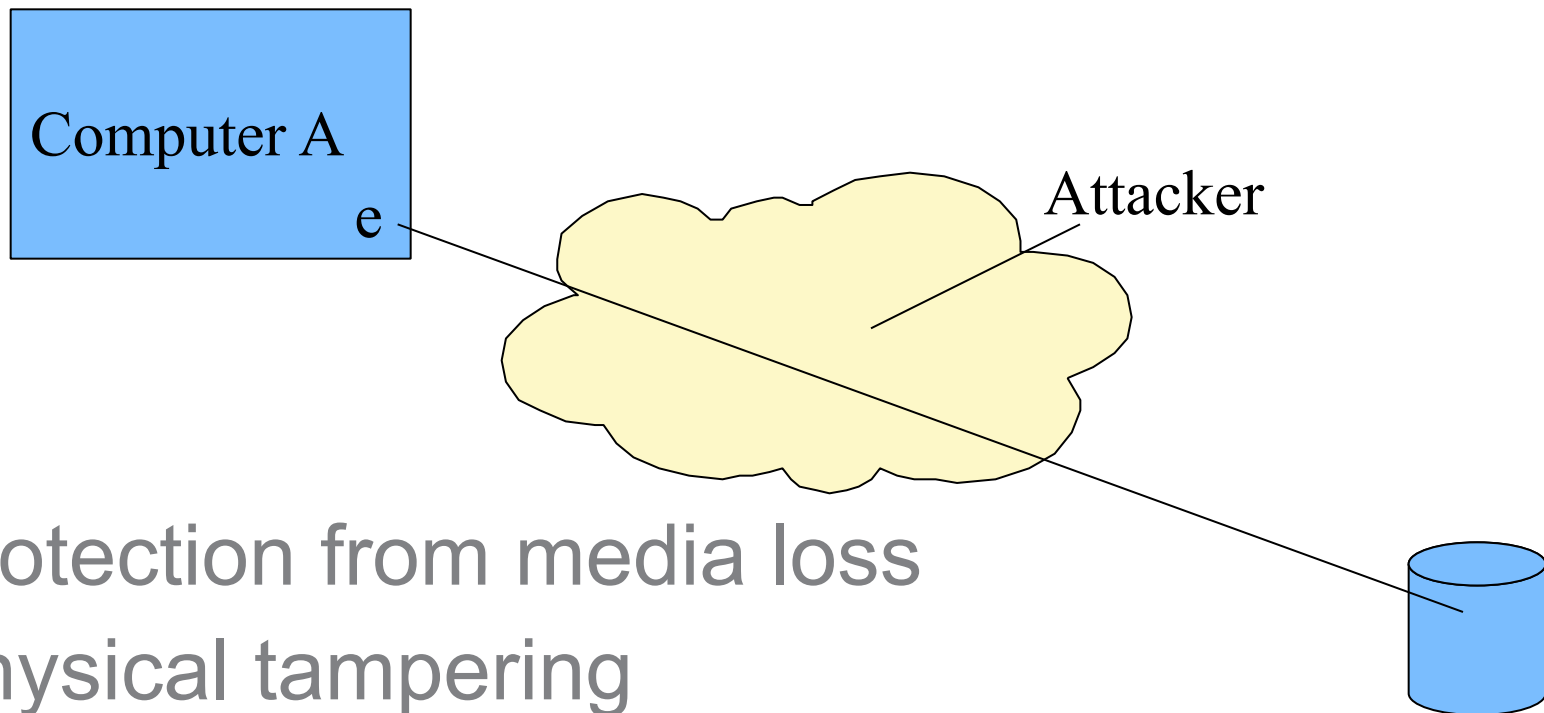


Protection from media loss  
Physical tampering

# Storage Configurations

---

## SAN, Fibre Channel



Protection from media loss

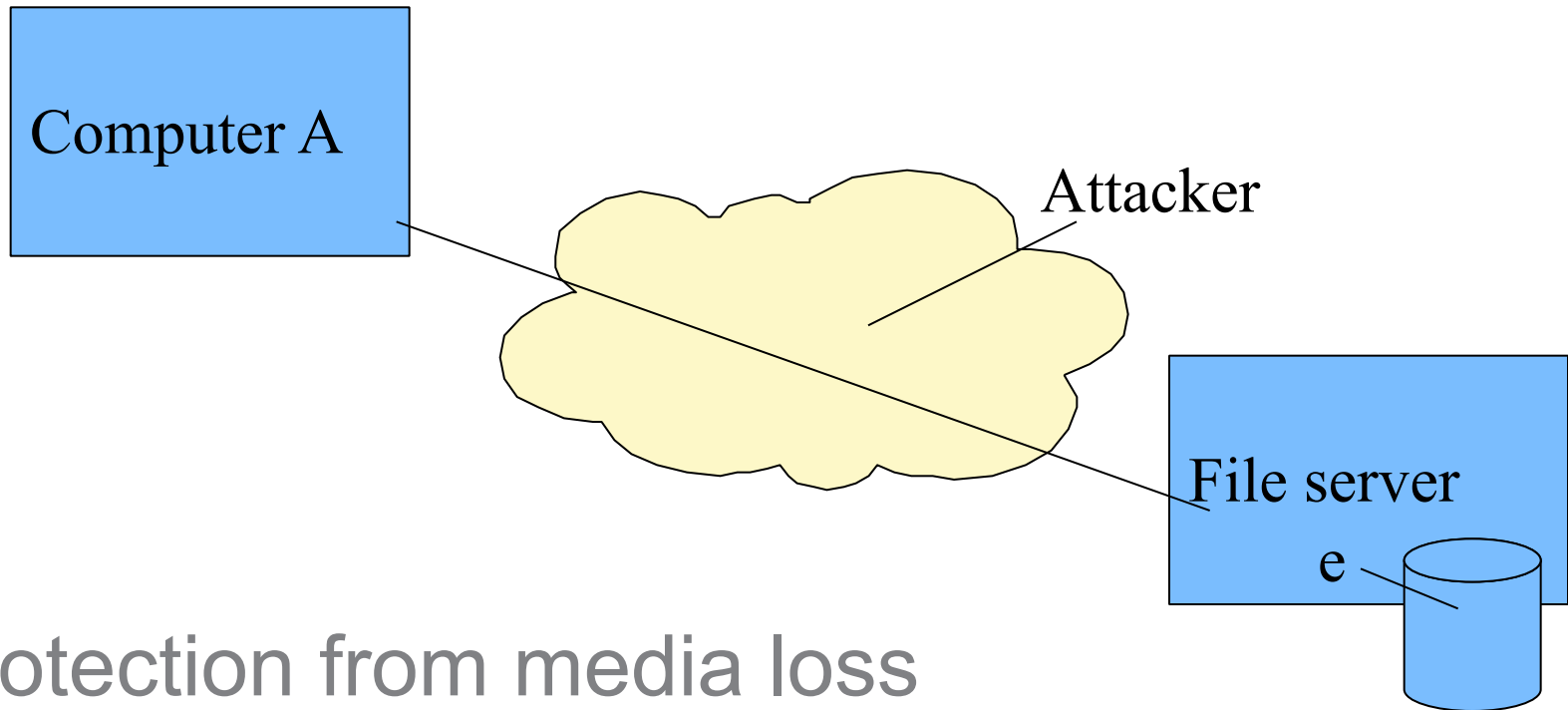
Physical tampering

Network Vulnerabilities

# Storage Configurations

---

NAS (NFS for Unix or CIFS for Windows)

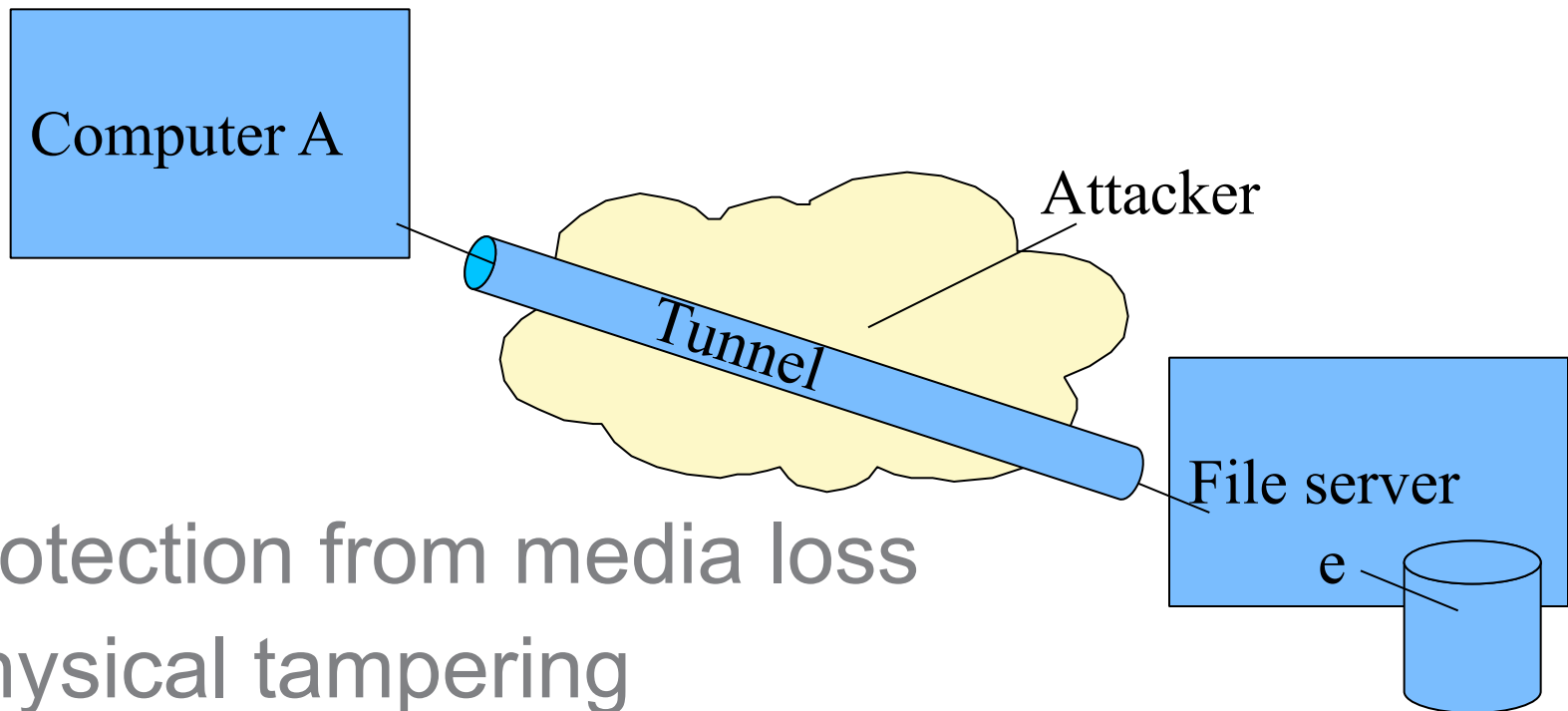


Protection from media loss  
Physical tampering

# Storage Configurations

---

NAS (NFS for Unix or CIFS for Windows)



Protection from media loss

Physical tampering

Network Vulnerabilities

# Storage Security vs Network Security

---

This presentation is focused on Storage

Storage can be considered a network

- With infinite latency

- D-H key agreement not possible

- Storage Reader may not exist when written

Requires OOB key communication

# Security Attributes of Secure Storage

---

## Privacy

- Algorithm and Birthday bounds
- Ciphertext feedthrough

## Integrity

- Malleability of ciphertext
- Cut and paste

## Authentication

- Key management

## Non repudiation

# Key Management

---

Requirements are simple

“Don't lose the keys”

“Don't give the keys to the wrong people”

Combine this with the OOB key requirement

Many organizations working on this

Companies, Standards, etc.

Vulnerability of passwords

Algorithms can not forget

# Existing Systems and Sample Attacks

---

## Existing systems

- Mac OSX Filevault

- Vista Bitlocker

- Tape encryption (various vendors)

## Future Systems

- Encrypted ZFS (OpenSolaris project)

- <http://opensolaris.org/os/project/zfs-crypto/>

# Mac OSX Filevault and others

---

## Algorithm and Birthday bounds

Leaks information after the birthday bounds.

64 bit block ciphers insufficient

## CBC implementation

No room for integrity field

Cut and paste

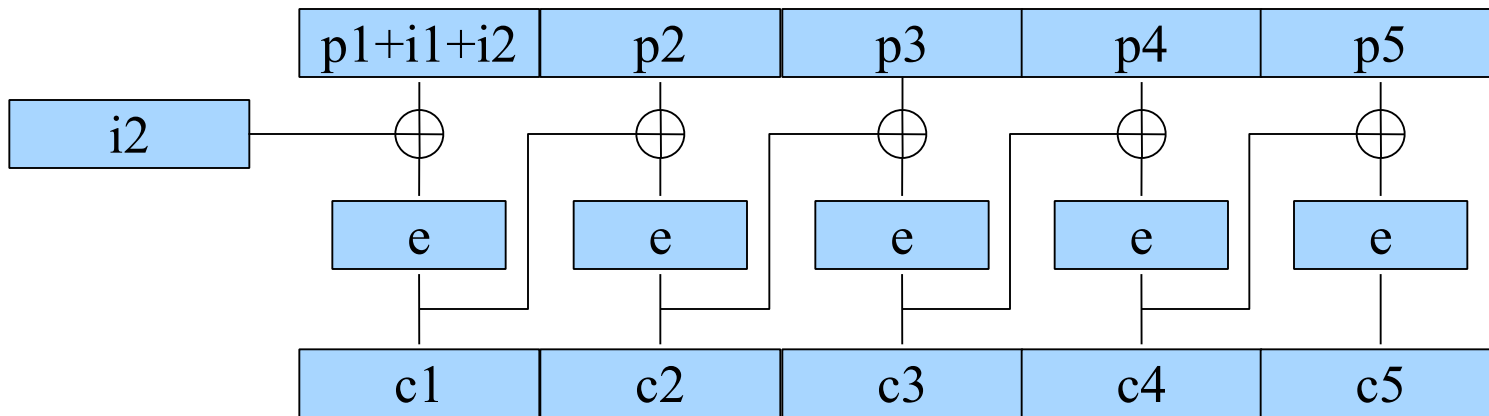
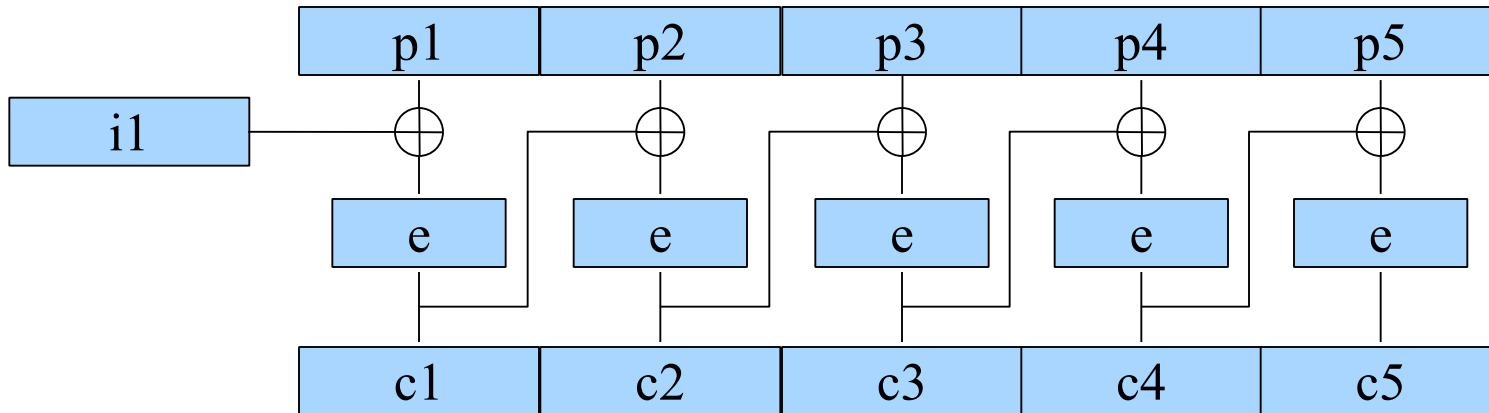
Malleability of ciphertext

Ciphertext feedthrough

Selective Replay

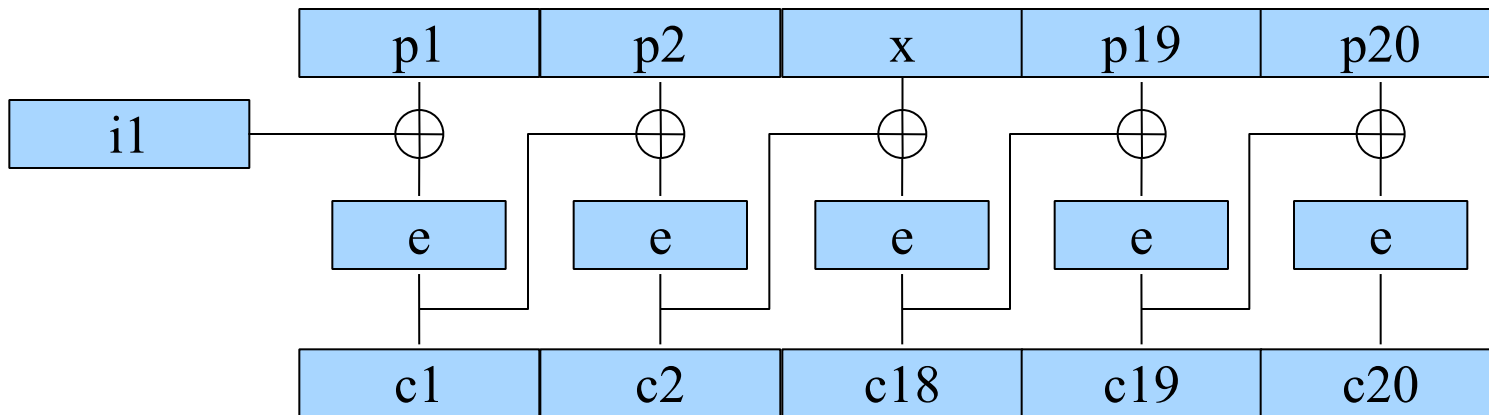
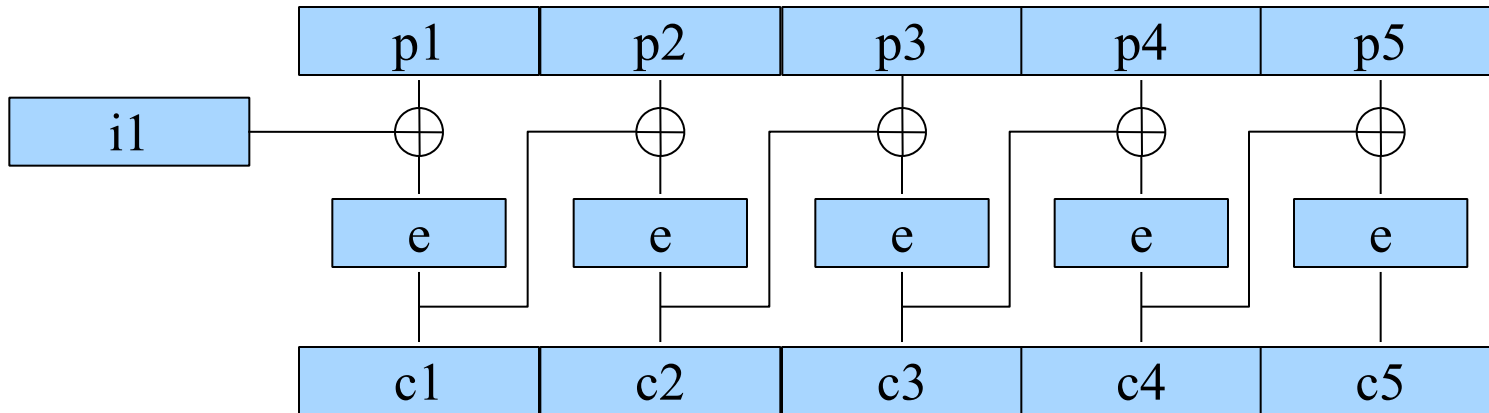
# Moving data

---

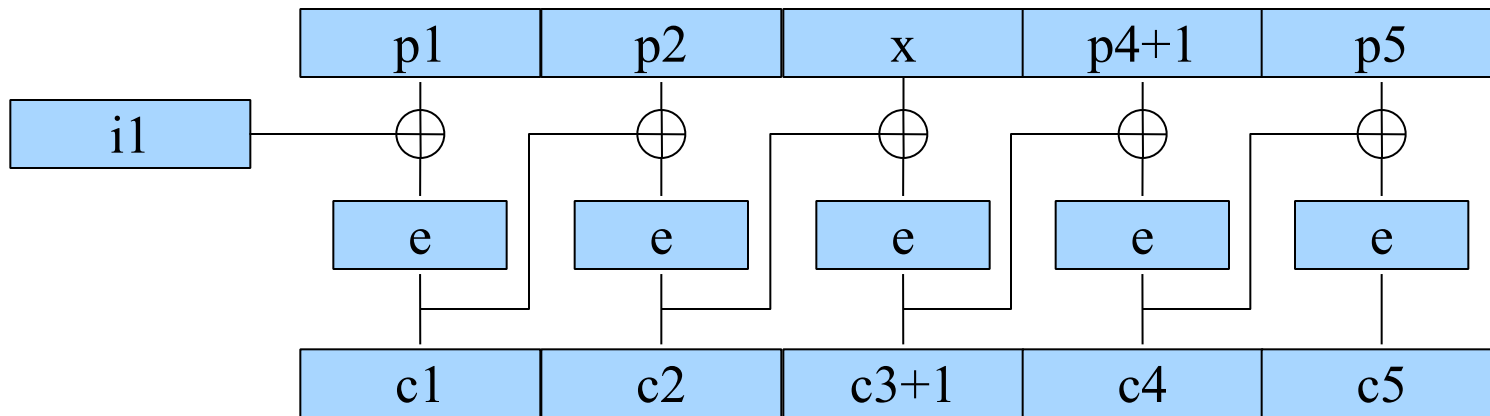
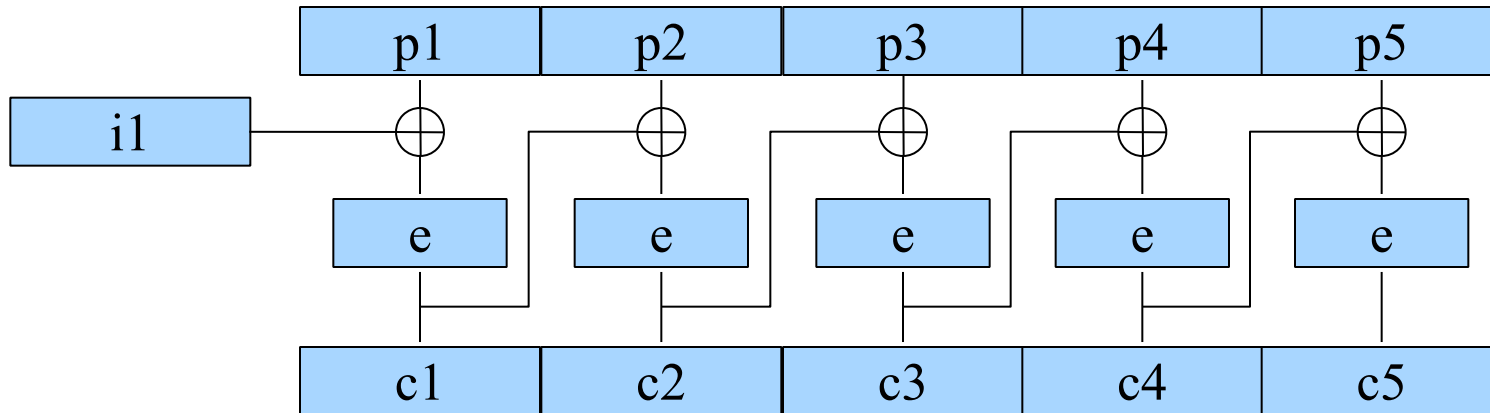


# Cut and paste

---

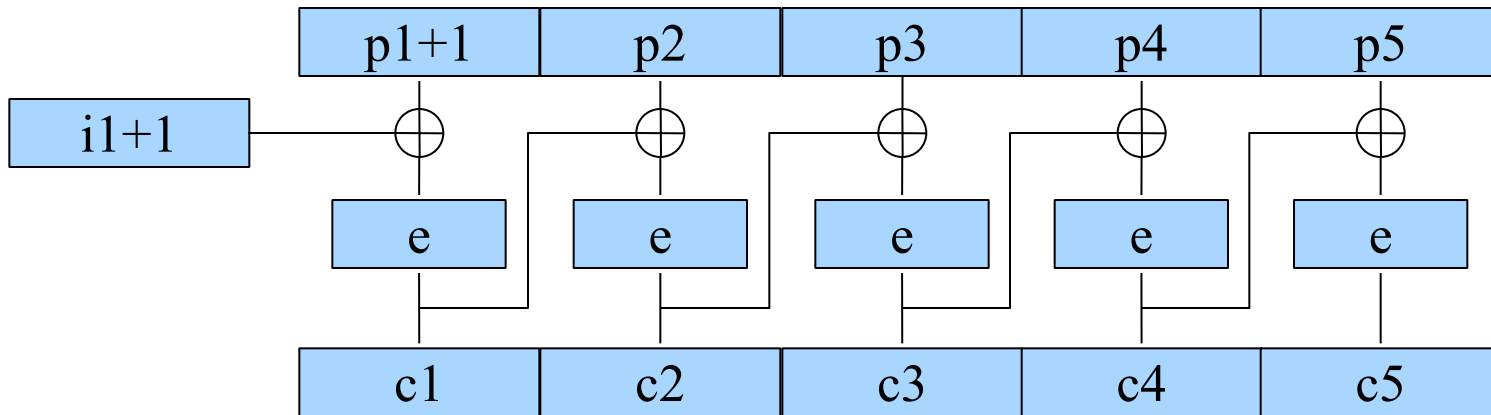
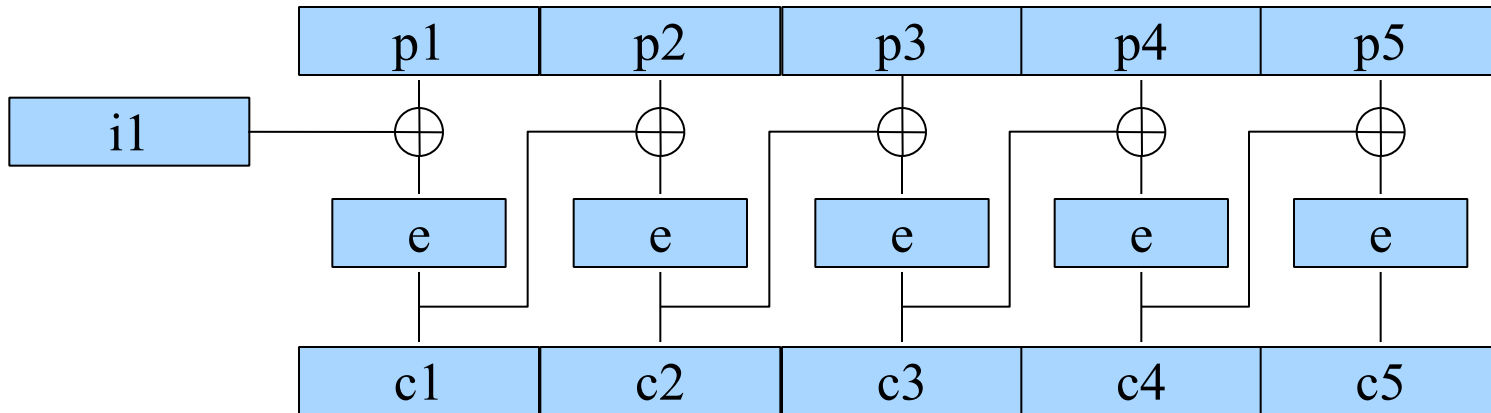


# Malleability of ciphertext



# Ciphertext feedthrough

---



# Vista BitLocker, P1619.0, P1619.1

---

## Tweaked block cipher

- Like adding public info to key, eg Sector number

- Still no integrity field

- Large block PRP

## Eliminates previous attacks

### Allows determining if data is returned

- Detect  $A \rightarrow B$  and then later  $B \rightarrow A$

### Replay of individual blocks (P1619.0)

### Replay of individual sectors (BitLocker, .1)

# Tape encryption

---

Tape offers variable blocksize

Room for integrity field

LTO, IBM, and Sun

Implement AES in CCM or GCM mode

All future tape drives will contain this feature

Similar to tape compression

# ZFS encryption

---

ZFS is a log structured file system

- Utilizing copy on write

- Data is not overwritten

- Data not just stored in sectors

<http://en.wikipedia.org/wiki/ZFS>

Room for an integrity field

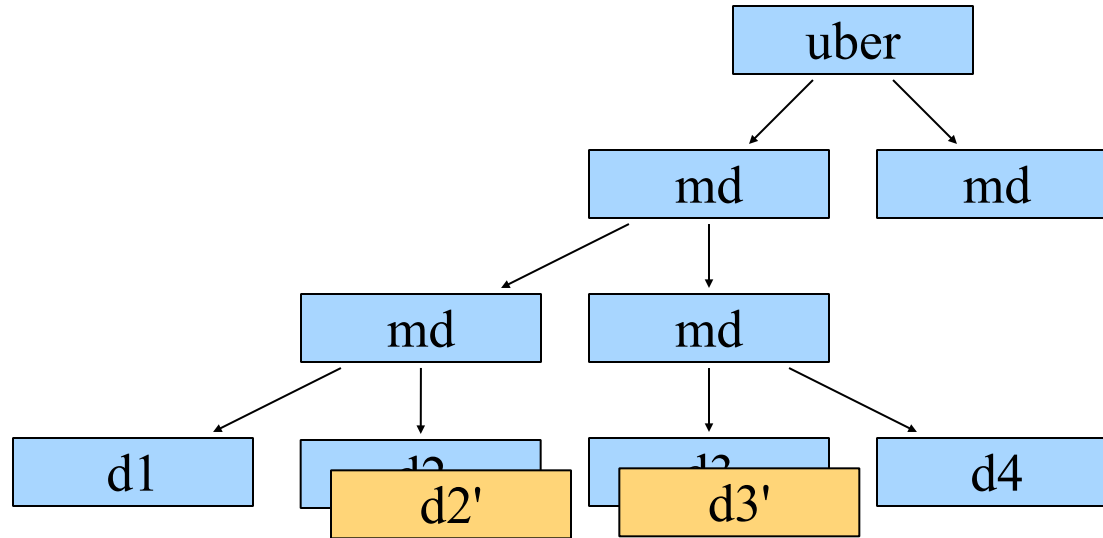
- Complete Merkle tree

- Validating the entire filesystem

- Hashes for level x stored in level x-1

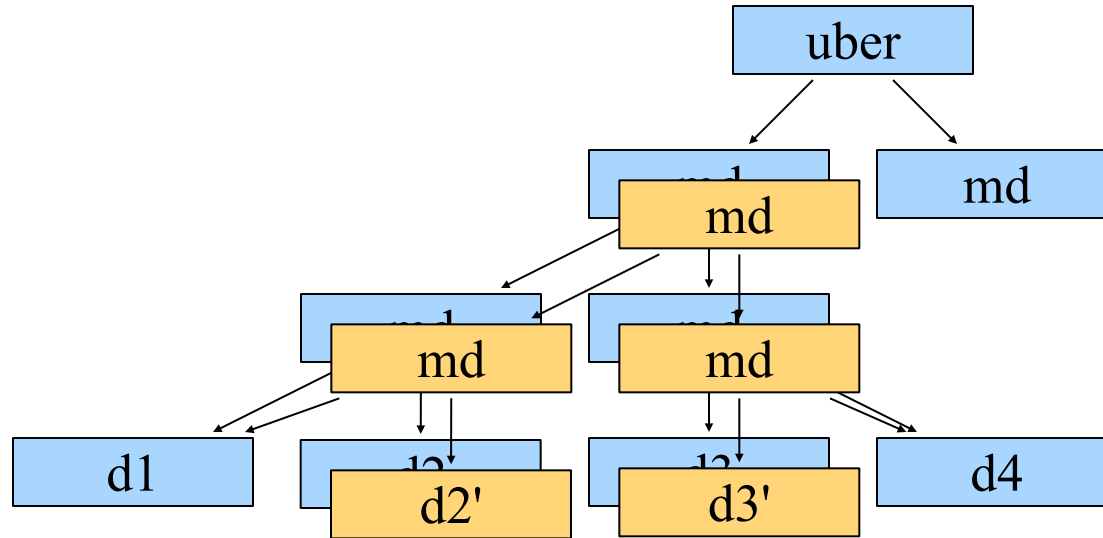
# ZFS tree

---



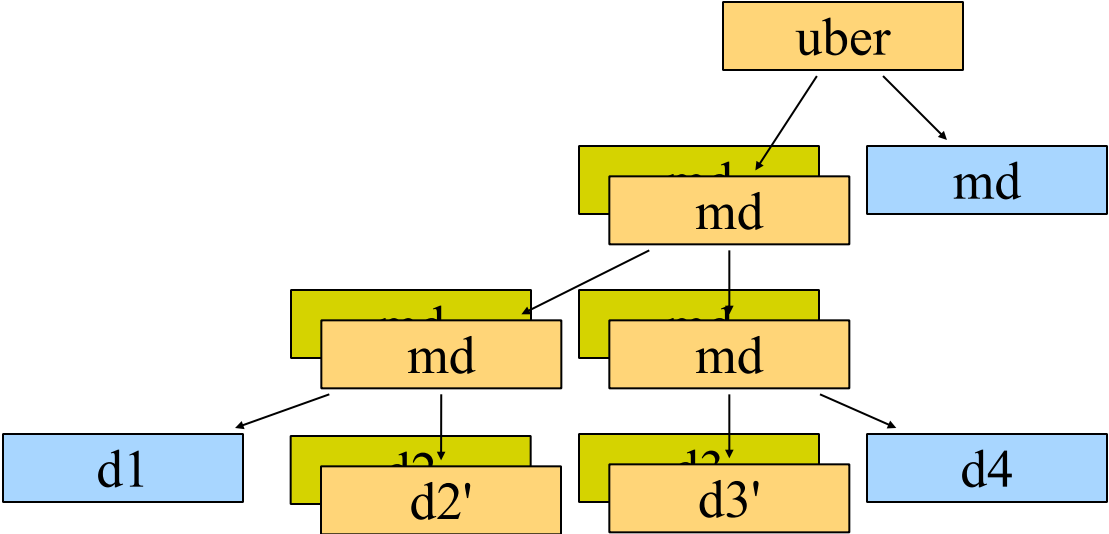
# ZFS tree

---



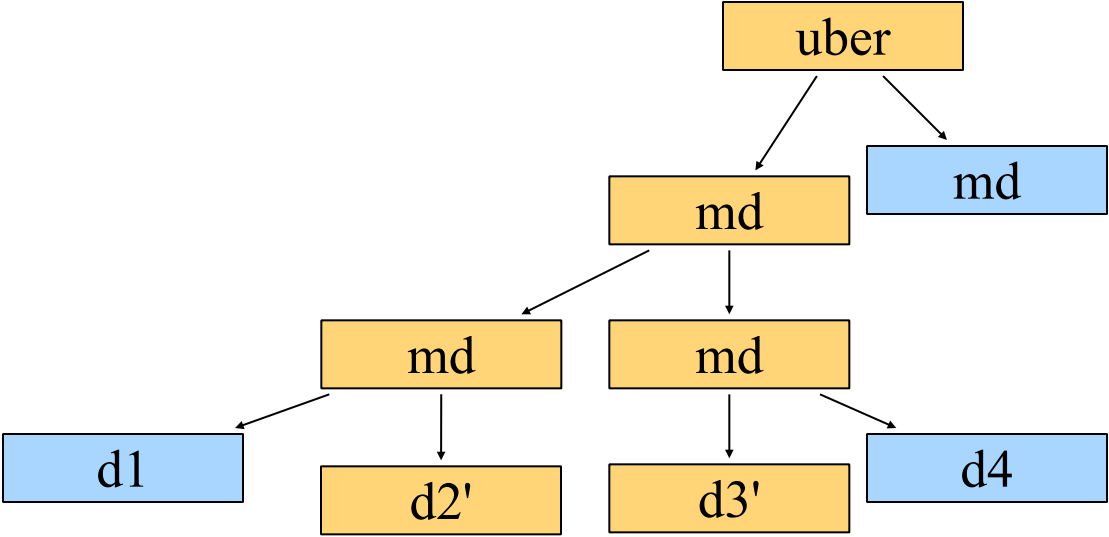
# ZFS tree

---



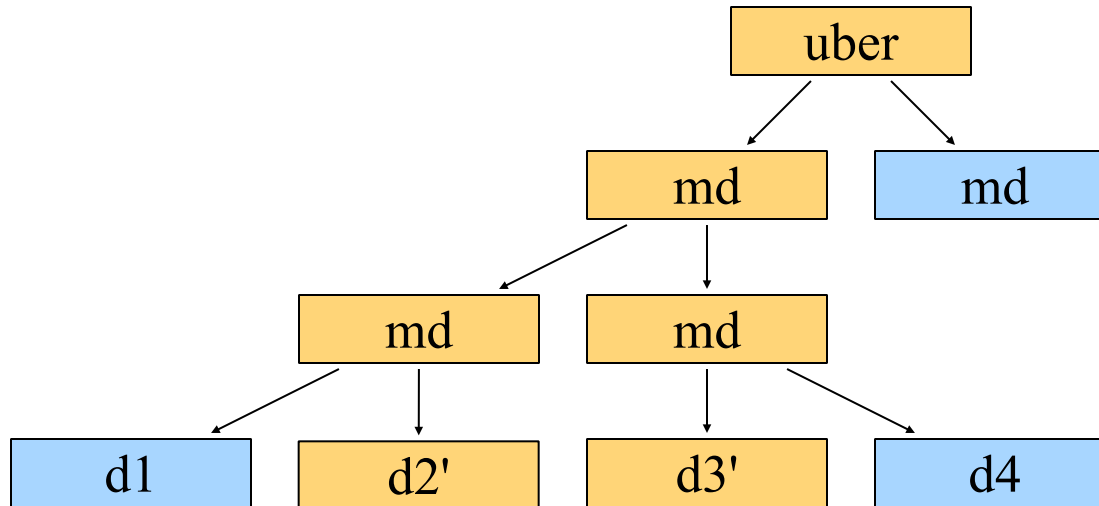
# ZFS tree

---



# ZFS tree

---



# ZFS

---

Overwriting a file 7 times does not erase the data

Encrypted data keeps hashes in the MetaData Tree

When the user is not logged in, the administrator can not see the data

Backup should be in the clear or under a separately managed key so that users are not vulnerable to key loss

---

	Cut/Paste/Move	Malleability	Feedthrough	Sector Replay	Data Return	Disk Replay
Filevault	✘	✘	✘	✘	✘	✘
Bitlocker	✓	✓	✓	✘	✘	✘
eZFS	✓	✓	✓	✓	✓	✘
eZFS/TPM	✓	✓	✓	✓	✓	✓
eTape	✓	✓	✓	✓	✓	✓

# Performance vs Trends in Computers

---

Measured AES, 100MB/s, on Laptop

This is only going to go up

Single disk performance 40MB/s

Relatively constant (until Flash)

First access has latency

Subsequent access access in RAM buffer

This level of performance is “free”

In the OS is “free”

“Security is an expectation, not a market”

# Long Term Prediction of Adoption

---

Computers are fast enough

OS vendors will add for free

Yes, there are country issues

At least password protected

There is no reason not to encrypt

***In the future, not encrypting your storage will be like using telnet instead of ssh***

# Areas for Future Research

---

Non-Repudiation

Secure and Reliable Human authentication

Affordable Tamper Responsive Hardware

Key management for machine hibernation

Encrypted boot

# Conclusion

---

Storage contains personal information  
Storage Security vs Network Security  
Security Attributes of Secure Storage  
Existing Systems and Sample Attacks  
Performance vs Trends in Computers  
Long Term Prediction of Adoption  
Areas for Future Research

---

Fin

