

Persistent Security

Jim Hughes

Fellow

Storage Technology Corporation

jim@network.com

<http://www.network.com/~hughes>

Security Breaches

- 73% Virus
- 54% Unauthorized use
- 25% Theft/destruction of resources
- 19% Resource leaks
- 19% Theft/destruction of data
- 14% Access abuse by authorized people
- 12% Unauthorized access by outsider
- 12% Hacking
- 7% Other

(Fire)Walls are insufficient

- Does not solve the hard problems
 - Insider Threat
- What is needed?
 - harden all hosts
 - Every host is its own firewall?
 - Strong human authentication
 - Anonymity is seldom needed within a company
 - Non-repudiatable audit trails
 - Deterrence
 - "Information Security"
 - Secure File Storage mechanism

Insider Threat

- **Rogue Employees**
 - Every PC is a sniffer,
 - Hack from the inside
- **Information Systems (IS) organizations are large**
 - 5% of the typical company
 - hundreds to thousands of people
 - These people can access your data many ways
 - Email admin - surf email
 - Backup Admin - surf your backups
 - Network admin - sniff network
 - File Server admin - surf your files
- **Employees are necessary**

SAN Security

- **Various Vendor items for Fibre Channel**
 - Soft Zoning
 - Hard Zoning
 - Login Authentication
- **Evolutionary approach**
 - Repeating many of the same mistakes
 - Re-inventing the wheel
- **Current state of the art**
 - 'Barbed wire fences and guns'
- **SANs fundamentally enable Storage Pooling**
 - What used to be in separate locked rooms

iSCSI

- Standard expects IPSEC
- iSCSI vendors relying on external boxes
 - Cost more than 2x the RAID controller and HBA combined
 - "Link encryptors are iron pipes that rats run through"
- Many networks will be uncovered
 - Not IETF standard
- Not End-to-End
 - Open at source (LAN) and destination (SAN)
 - Open on the storage
 - Solves the problem over the WAN
- Expectation?
 - Eliminates the barbed wire fences

Secure Information storage

- **Two Ways**

- **Secure the entire enterprise**

- Many times larger and more complex than securing a single system
- Becomes harder as the organization gets larger

- **End to End security**

- Data is protected from the producer to the consumer
- Covers Networks, Backups, SANs, File Servers
- Solves the insider threat

Strategy

- Solve the hard problem
 - Insider Attack
 - End to End security
- Easier in the long term than 'Security Everywhere'
 - More effective
 - More transparent
 - lower cost

Security of the information at rest

- End-to-End Security
 - The disk is not an end.

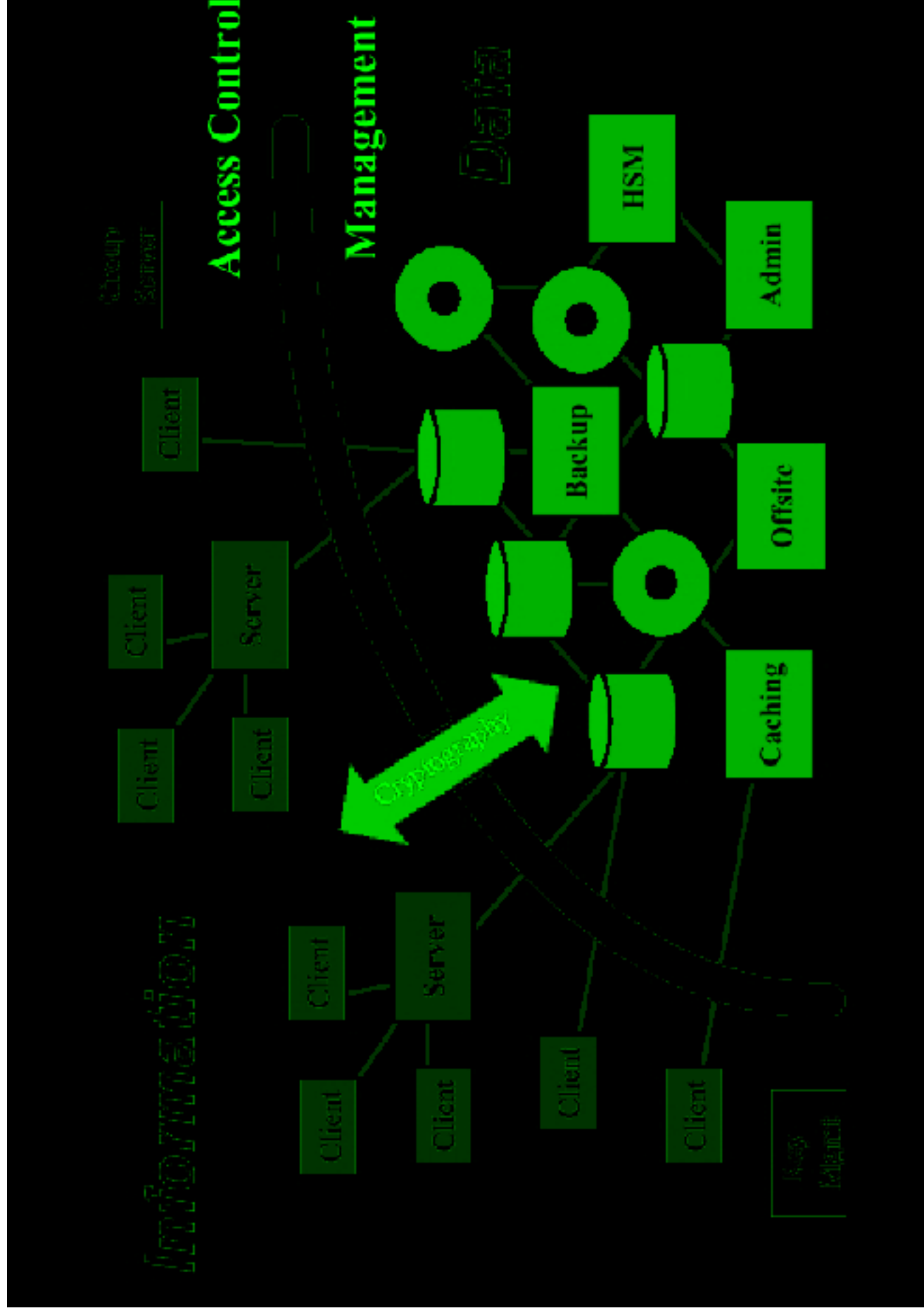
Research

- Why not application?
 - Authentication wars
 - Not secure
- SAN Encrypted Volumes
 - Disk
 - Tape
- Virtual WORM
 - Guaranteed correct
- Global File System?
 - Encrypted File System

Encrypted File System

- Independent of the underlying file system
 - Cryptographic File System, CFS, Matt Blaze
 - Shared files require shared keys
 - Satan File System, SFS, CMU
 - Interesting demonstration, Lib.c modifications
 - Distributed File System, DFS, IBM
 - Security is a network problem
 - Networked Attached Secure Disks, NASD, OBD, SCSI-4
 - File system has the master keys
 - Encrypted File System, EFS, Microsoft Windows 2000
 - :^(
 - Secure File System, SFS, STK
 - www.securefs.org

Secure File System



Encrypted Media

- **Not a new concept**
 - Loop driver - Ted Tso
 - Encrypt near host, not disk
 - Veritas encrypted backup
- **1GB/s encryption feasible**
- **Method to encrypt an entire volume**
 - Transparent to the original host
 - Boot through
- **Destroy the key**
 - Destroy the data - a good thing
- **Needs standards**

Long Term Storage Risks

- Existing way to lose your backup data.
 - Lose, break tape
 - Lose the drive
 - Lose the restore program
- Encrypted Storage
 - Lose, break the key
 - Lose the algorithm
- Encryption increases an already non-zero risk
 - What does it solve
 - What is your information worth to your adversary

Common Criteria

- **Assessment of all Information Security products**
- **Needs to separate from the storage device**
 - Will never successfully evaluate a complex storage system
 - Large global file system
- **Storage encryption devices can be evaluated**

Conclusion

- Defining a boundary is hard, the threats are real
 - Externally and internally
- 'Security Everywhere' is neither
 - More security systems the higher the risk one is bad
- Encrypted media
 - Solves real problems
 - Reasonable
 - cost - time, money
 - risk - key management
- Global File System
 - Needs an independent security mechanism