HDD Based Full Disc Encryption

Dave Anderson
Seagate Technology, M/S SHK233, 1280 Disc Drive
Shakopee MN 55379-1863, Ph: +1-952-402-2991
e-mail: david.b.anderson@seagate.com

Presented at the THIC Meeting at the Sony Auditorium, 3300 Zanker Rd, San Jose CA 95134-1940

February 28 – March 1, 2006

HDD Based Full Disc Encryption

Dave Anderson
Seagate Technology

Full Disc Encryption - Momentus FDE

- **Purposes**
  - Protect data from exposure due to equipment loss,
  - Enable instant, secure erase of HDD

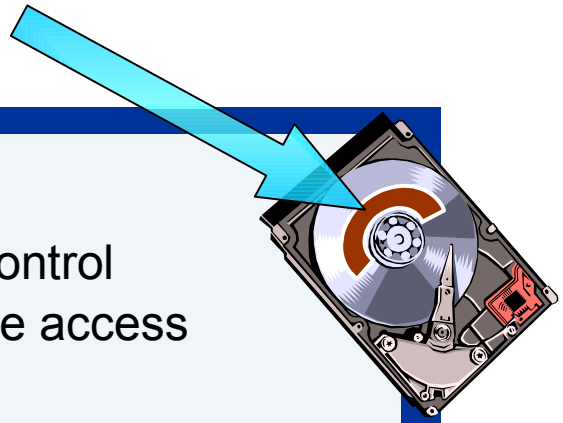
- Government Standard based encryption
  - Universally adopted 3DES algorithm
  - Dedicated engine for full interface speed encryption
  - Key protected on media
  - Key inaccessible using standard READ/WRITE commands

- Closed encryption device
  - Key generated in drive during manufacturing
  - Encryption cannot be turned off
  - Key never leaves drive
  - Huge bandwidth advantage when used on drives in parallel

FDE – Driven by New Statutes

- *Document Disposal provision of FACTA in effect as of 6/1/2005*
  - *Co's required to destroy, not just dispose of sensitive consumer data*
  - *"destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed"*
- *CA SB1386 (21 states now have legislation)*
  - *Co's must notify consumer of data loss*
  - *Liable if best practices not employed to protect data*
  - *Safe harbor for encrypted data*
- *HIPAA, GLB already have destruction provisions*
- *New law in Japan – in effect as of 4/1/2005*
  - *Obliged not to provide personal information with any third party without the consent of individuals (i.e. do not lose information)*
  - *NEC, Hitachi developing HDD-less laptops to avoid violation*

Why Security in the HDD



- **3 Simple reasons**
  - Storage for secrets with strong access control
    - Inaccessible using traditional storage access
    - Arbitrarily large
    - Uncircumventable gate to access
  - Unobservable cryptographic processing of secrets
    - Processing unit united to storage
    - Secrets can be cryptographically processed in secret
  - Custom logic for faster, more secure operations
    - Inexpensive implementation of modern cryptographic functions
    - Makes feasible complex security operations

FDE Functionality

- **Momentus FDE Encrypts/Decrypts the Data for:**
  - Write/Read Buffer
  - Write/Read Sector
  - Write/Read Sector EXT
  - Write/Read Multiple
  - Write/Read Multiple EXT
  - Write/Read DMA
  - Write/Read DMA EXT
- **All other commands pass data in the clear**

FDE Keys and IDs

- **Security ID (SID) –Used to verify possession of the drive**
  - Printed on drive label
    - Changeable by someone who knows SID
  - Random number generated at the factory
  - Used to control dCards and drive operation
- **Master ID (MID) – This is the master ID for the drive**
  - Required for disc erase, User ID override and key escrow
  - Used by IT departments to control drive and override individual users
  - Set to SID after secure erase, key restoration, and initiation of Drive Trust functions
  - Not stored in the clear on the drive
- **User ID (UID) – User's password (derived from password or other user authentication mechanism) for daily access to the drive and its data**
  - Can be overridden by using the MID
  - Changeable
  - Not stored in the clear on the drive
- **Encryption Key – The key that is used to produce the encrypted data on the disc**
  - 3DES symmetric encryption
  - Random number generated by FDE in the factory
  - 192 bits
  - Not stored in the clear on the drive

FDE Deployment

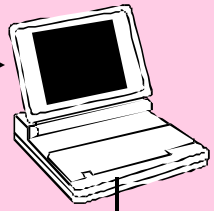
SID initialized and printed on label

Encryption key initialized and stored securely

Encryption is on

User ID Not Initialized

Drive Sold



SID moved to system case

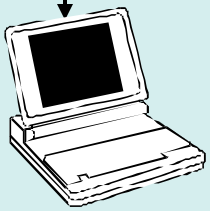
Secure erase (generate new encryption key)

Possibly add optional features:

- biometrics for UID
- enterprise key management

System Manufacturer

System sold



IT changes SID

IT saves old SID if restoration to original state is desired

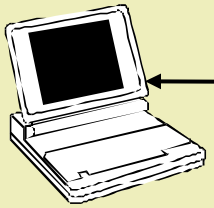
IT sets a default UID

IT optionally escrows new SID

IT optionally escrows Encryption key

IT dept.

System Delivered to end user



User powers on, enters UID

User changes UID

Uses system normally

End User

Customer

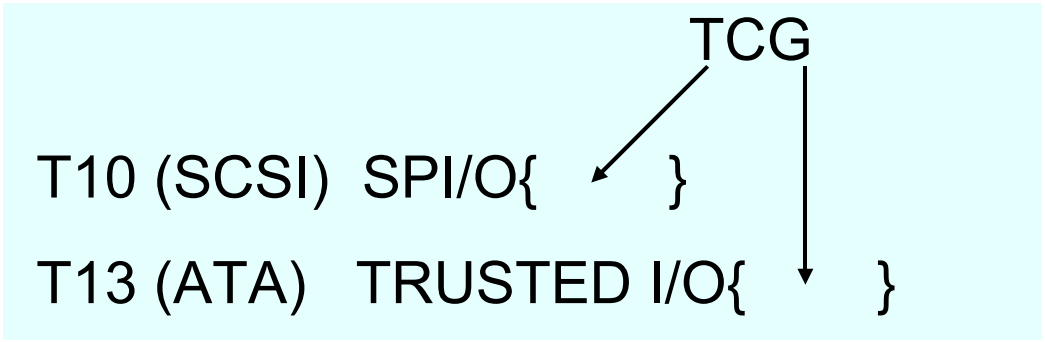
Standards Strategy

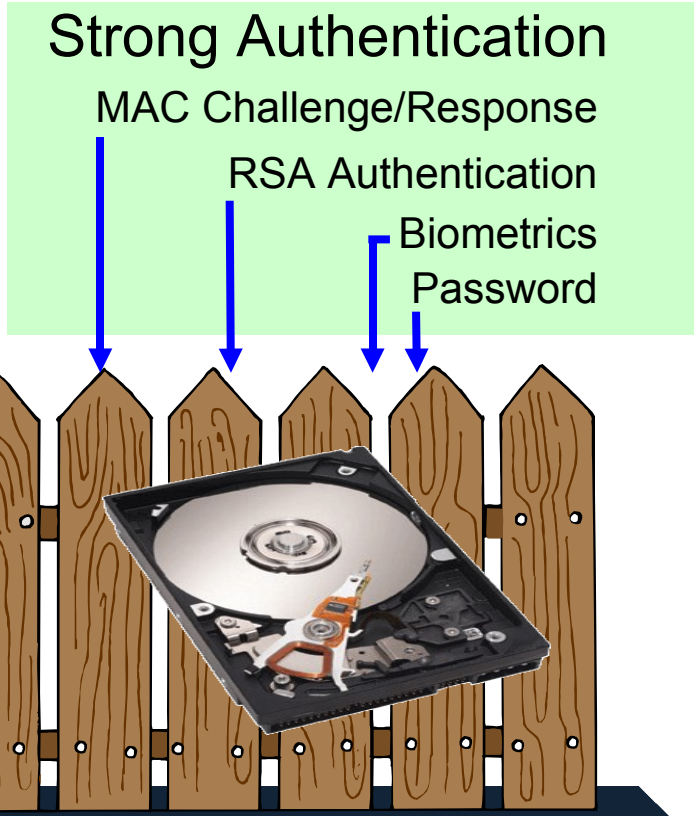
Security experts to develop security access method (TCG)

Storage experts to develop transportation (ATA & SCSI)

Get them to work together

Make usable by other security applications (Protocol ID: TCG, …..)





SECURITY PROTOCOL OUT

SECURITY PROTOCOL IN

TCG Use Cases

Enrollment and connection

Protected storage: impervious to unauthorized access

Locking and Encryption

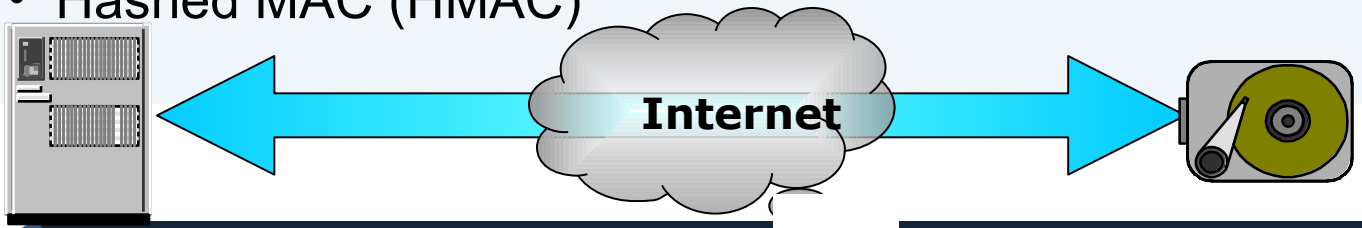
Forensic Logging

Cryptographic Services

- Hashing: SHA-1, SHA-256
- Symmetric encryption/decryption: AES-128
- Public key encryption/decryption: RSA, ECC
- Random number generation
- Secure messaging

Root of Trust w/ Strong Access Control

- **Root of trust for secure communications**
  - Can establish secure communications with another trusted endpoint
  - Communication can pass through any untrusted environments
    - OS
    - BIOS
    - Internet
    - Cell network
- **Access Control**
  - Password
  - PuK with Certificate Chaining
  - Message Authentication Code (MAC)
  - Hashed MAC (HMAC)



FDE = Value

- *Recent data loss headlines emphasize the need for encryption*
- *FDE cannot be turned off*
- *Component of regulatory compliance*
- *Offers instant secure erase*