HDD-based Security
SMR Recorded HDDs

Dave Anderson, Seagate Technology
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
Industry standard protocol to access security services, methods & data. Supports secure communication & strong authentication.

Uncircumventable access control
Signed firmware
**AES encryption in ASIC**
Cryptographic methods:
AES, RSA, RNG, SHA-1, SHA-256…

High Quality RNG partly derived from media signals

Security Providers = Logical “SmartCards”
Each securely issued & isolated from all others

© 2011 Seagate Technology. All rights reserved.
Cryptography

Asymmetric encryption
  • RSA 1024 => 2048
  • EC under consideration

Symmetric encryption
  • Done in hardware for full interface performance, zero latency
  • FC, SAS will have dual crypto engines, one for each interface
  • AES-128 & AES-256
  • =>Block chaining, LBA seeding
  • Support for non-512 multiple block sizes & Protection Information (PI)

Hashing
  • SHA-1 & SHA-256

Random number generation
  • Head noise-based RNG
  • Adding hardware RNG
HDD security services can establish secure channel

- Can pass through untrusted BIOS, OS, app, WWW
- Can create session keys & secure sessions
- Can issue and respond to challenge/response sequences
- Supports PKI signing and verification
- Supports MAC & HMAC
- Has X509 certificates for authentication
Areal Density Growth

- Late 1990s – superparamagnetic limit demonstrated through modeling
- Perpendicular expected to extend to ~1 Tb/in²
- Additional innovations required at that point
  - heat-assisted recording
  - bit patterned media recording
- Areal Density CAGR 40%
- Transfer Rate CAGR 20%
Challenge: Increasing Capacity

Higher capacity comes from higher areal density

• Blocks smaller, more susceptible to errors
• Spacing tighter, raising risk of fringing effects
• New technology to enable higher areal density:
  • Patterned media
  • Heat assisted magnetic recording
  • Great technical difficulty and risk to implement
  • Capacity growth will slow significantly until at least one is in place

Enter Shingled Magnetic Recording (SMR)
SMR: A New Hope for AD Growth

SMR: Shingled Magnetic Recording - band(s) of disk with:

- Within a band only sequential write forward capability
- Blocks in these areas cannot be updated
- Full random read support
- Could be multiple or lots of such bands per drive
- Some area of the disk may be organized with traditional random Read/Write capability
SMR - Some Advantages & Questions

Advantages

• An obvious candidate path for AD growth
• SMR - relief for the head manufacturing variation issues

Questions

• What applications can use SMR?
• What system changes will be needed?
  • How should bands be sized?
  • What is relation between SMR bands and traditional R/W area?
• Will those result in a storage device with sufficient application?