



# DRM Building Blocks in Secure Disk Drives

Laszlo Hars, Robert H. Thibadeau

*Seagate Research*

January, 2005

**Seagate**

We turn on ideas



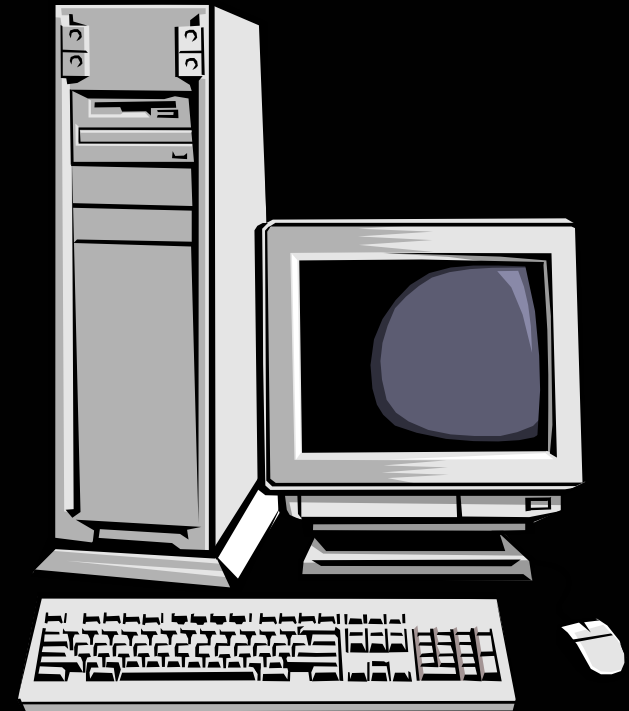
# Outline

- Research project
- Standards: Trusted Computing Group, SNIA, IEEE SISWG...
- Why DRM in disk drives?
  - Open / Closed systems
  - Ubiquitous disk drives
  - Free computing capacity
- Security in disk drives
  - Data protection
  - Rights/policy management
  - Low level functions
- Extensions
  - File system aware disk drives
  - Auxiliary functions

# Open Systems

## *Computers with*

- Communication ports
  - Ethernet/wireless Network
  - Parallel, serial ports, USB
  - FireWire, IEEE1394
  - SCSI, SATA, ATA...
- Removable storage
  - Optical: CD, DVD...
  - Magnetic: disks, tapes, Floppy, Zip drive...
  - MO disks
  - Solid State: FLASH

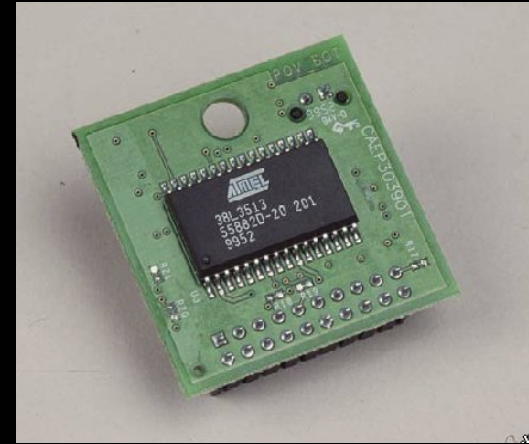


# Don't trust the Host

- Malware (virus, worm, Trojan...)
- Information leak
  - Memory
    - At exception, interrupt, context switch: heap, stack, cache
    - Data retention
    - Fault injection
    - RAM data as file slack
    - Search/Indexing services
  - Disk (temporary files, swap files, hibernate area, file slack, bad sectors...)
- SW Bugs (buffer overrun, error conditions...)
- HW: Debugger, bus-logic analyzer

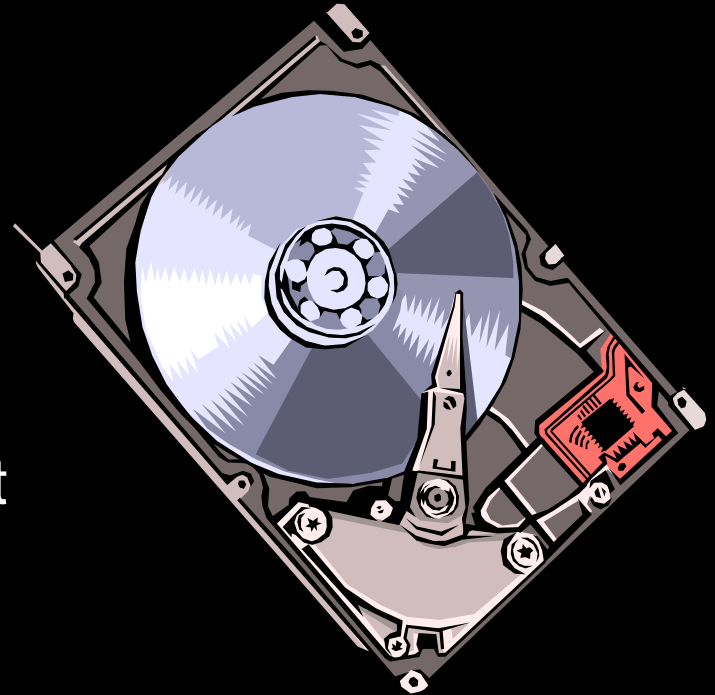
# Securing open systems

- Trusted component
  - TCG – TPM, Secure peripherals
    - Keyboard (no password sniffing)
    - Readers for Smartcard, Fingerprint, Security token...
    - Disk drives
- Trust from boot-up
  - Verify BIOS
  - Verify OS-core
  - Check loaded SW...
- Tamper resistant SW
  - Slow, large, expensive



# Closed Systems

- No foreign SW
  - Authenticated, read only FW
- Restricted interface - port
  - Fixed command set, data format
- Protected internal buses
  - Single chip
  - Multi-chip *module*
- Physically separate data and program memory
  - No buffer overflow-type attacks



# Disk drives everywhere

- In consumer electronic devices
  - Everywhere
  - New application scenarios
- New business possibilities
- New challenges
  - Protection of the rights of the owner of digital content
  - Data owned by third parties
    - Transferred
    - Stored
    - Played back...



# Advantages of DRM support in Disk drives

- Powerful computational engine inside
  - For internal data processing
  - For control functions
  - Not constantly fully utilized
- Closed system
  - Physically: data buses, memory lines are not exposed
  - Fix firmware, no external code executed
  - Host communication: Fix command set, data format
- Huge hidden, protected storage
- Secure (authenticated) firmware ***update***
  - Support changing requirements
  - Renew-ability: if security is breached, new standards...

# General Disk Data Protection

## –In transit

- Against traffic analysis
- Data modification
- IEEE SISWG: long-block encryption tweaked by location

## –At rest

- Encrypted: Disk-erase by key-destroy (eNova, Stonewood)

## –Partition dependent encryption

- Originated from SCSI'86
- Contiguous LBA ranges with one key encrypted
- Authenticated in BIOS (trusted)
- Separation of users, applications

# Multimedia Content

- In a secure form
  - Encrypted, scrambled/distorted
  - With key dependent algorithm
- Attached rights – describing allowed operations
  - Disk may not enforce policy
  - Provide information, building blocks for DRM
- Source – sink securely exchange keys
  - Source: Website selling usage rights
  - Sink: Secure video or sound **card**, game **console**, SW or CE **player** (music, video, image, text)...

# Secure Disks

- Master encryption key in the electronics
- User-, content- keys encrypted on disks
- Preloaded certificates, preset rules, rights
- Potential Disk-Command extensions
  - Manage access rights
  - Setup keys, return key handle
  - Erase key specified by handle
  - Establish session (transport) keys
  - Key export, import in wrapper
  - Designate LBA ranges for transparent encryption
  - Encrypted data send, receive
  - Re-encrypted data send, receive\*
  - Hidden storage, retrieval...

# Re-Encryption

## –The Host

- Does not know the keys
- Facilitates the communication between trusting parties

## –The Disk

- Buffers content
- Provides secure (encrypted) storage (server, library...)
  - For many sink devices, with keys directly from the content owner
- Provides hidden storage
- Provides encryption engine
- Re/encrypted data transfer
- Manages re/encryption keys

# Low level Tools provided on Disk

## – Monotonic Counter

- for logging
- for preventing replay (nonce)
- not for time dependent DRM policies

## – Secure time

- Battery backed-up RTC
  - heat, vibration = battery unreliable
- Imported secure time – trusted/non trusted time mode
  - drive nonce → time server, time + nonce signed by PK → drive

## – Physical Random Number Generator

- For nonce generation, Session keys, DH key exchange...
- Attacks: Side channel leakage, signal / fault injection...
- Defense: Shield, Duplicate / compare, On-line tests

# File System aware Disk drives

- **Full** FS handling: OSD (SNIA)
  - File attributes
  - Optimal file allocation
  - Authentication, Privacy
- **FS extensions**
  - Stash storage
    - Extensions to existing disk interface
    - Nonstandard host communication
    - Hidden/Reserved space: Fix or Resizable
- Drive can-
  - Generate signatures, verifications
  - Compute fuzzy extractors, data fingerprinting
  - Verify digital watermark
  - Handle attached information (content database)

# Attacks

## –Host/SW attacks

- Key search, break crypto, exploit protocol weaknesses

## –HW attacks

- Passive (eavesdropping)
  - Head wire is exposed
  - Spin stand [encryption chip at the head is not foolproof]
- Side channel leakage
  - Power, timing analysis, EM radiation
- Active
  - Data alteration: delete, insert, rearrange...
  - Fault injection: heat, cold, electrical, radiation...

# Auxiliary Functions

- In-drive digital watermark detection
- In-drive digital watermark insertion
- Content fingerprint computation
- Content information database management
- Fast search mechanisms, background indexing services (SCSI'86)
- ...
- Your ideas?