



DRM Building Blocks in Secure Disk Drives

Laszlo Hars, Robert H. Thibadeau

Seagate Research

January, 2005

Seagate

We turn on ideas



Outline

- Research team effort
 - Seagate participates in standards groups:
Trusted Computing Group, SNIA, IEEE SISWG...
- Open / Closed systems
- Ubiquitous disk drives
- Security in disk drives
 - Data protection
 - Rights management
 - Low level functions
- Extensions
 - File system aware disk drives
 - Auxiliary functions

Open systems

Computers with

- Communication ports
 - Network
 - USB
 - FireWire
 - SCSI, SATA, ATA...
- Removable storage
 - CD, DVD
 - Magnetic tapes
 - Floppy, Zip drive...

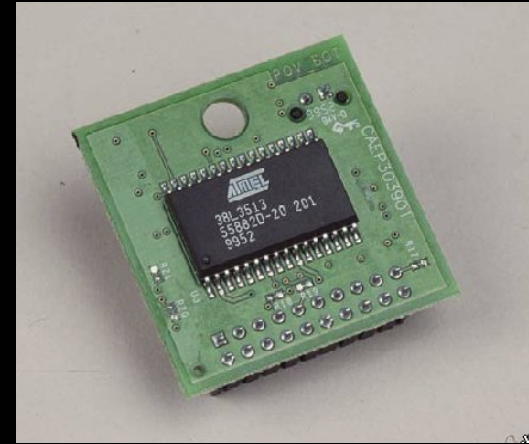


Don't trust the Host

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

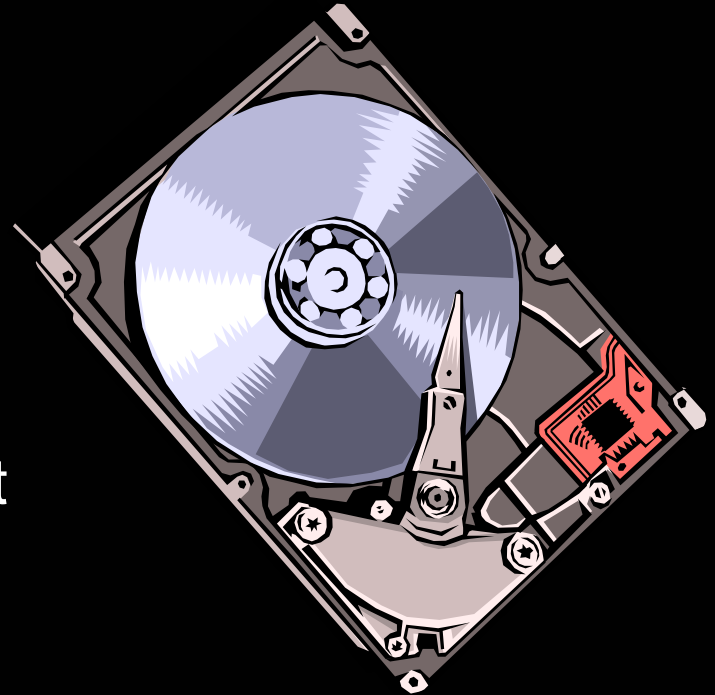
Securing open systems

- 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 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

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 exchange keys directly
 - Source: Website selling usage rights
 - Sink: Secure video or sound card, game console, player (music, video, image, text)...

Secure disks

- Master encryption key in the electronics
- User-, content- keys on disks
- Preloaded certificates, preset rules
- Potential Disk-Command extensions
 - Manage access rights
 - Setup disk 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
 - 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, crypto breaks, 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 detection
- Content information database management
- Fast search mechanisms, background indexing services (SCSI'86)
- ...
- Your ideas?