Content Protection for Recordable Media

Florian Pestoni
IBM Almaden Research Center
Why content protection?

- Shift from physical to digital distribution
- Content is licensed, not sold
- Digital content resides in potentially “hostile” environment
Can copyright infringement be prevented?

No, but...

- It can be discouraged
  - Self enforcement
  - Inconvenience
- Infringers can be prosecuted
- $5 lock protects $1000’s of property
It is Not About the Cryptography...

• Thought experiment:
  – Movies'R'us.com has just invented a novel compression technique for video
  – They get a strong patent on the technique
  – They license the technique for prerecorded DVDs, and require players to verify usage rights
  – Finally, they give the studios "third party beneficiary rights" which gives them status in court to sue infringers

• A complete, logical, copy protection scheme

… it’s about the license
Global secret schemes

- Once broken, *all* content is exposed to *everyone* at once

- Weakness in:
  - Thought experiment just described
  - CSS (DVD)
CPRM

- Jointly developed by “4C”: IBM, Intel, Matsushita and Toshiba

- Currently announced for: Secure Digital (SD) card, DVD-RAM/R/RW

... and its cousin CPPM

- DVD-Audio
Goals

• Protect stored content from simple replication
• Trace and revoke non-compliant devices
  – Renewable security
• Survive multiple “hacking events”
• Practical
  – Storage
  – Processing
Algorithmic lineage

• Broadcast encryption
  – Fiat and Naor, Crypto ’93

• Tracing traitors
  – Chor et al., Crypto ‘94
Elements of CPRM

- **C2 Symmetric cryptosystem**
  - Efficient implementation in hardware

- **Media Key Blocks**
  - MKBs are recorded on the media

- **Device Keys**
  - Are stored at the players
Licensing

• All elements must be licensed from licensing center (License Management International, LLC)
  – C2 “S-boxes”
    • To implement compliant players
  – MKBs
    • To CPRM-enable media
  – Device keys
    • To be able to play and record CPRM-protected content
• Small fees associated with the keys and MKBs
CPRM at work

Device Keys

Process MKB
- Km
  - Media key

One-way
- Kmu
  - Media Unique key

Decrypt
- Kt
  - Title key

Decrypt

Media Key Block
- ID_{media}
- E_{Kmu}(Kt)
- E_{Kt}(content)

Content
Device Keys

• A scheme consists of a large matrix of random keys
  – $K_{i,j}$ where $0 \leq i < R$, $0 \leq j < C$
• Each device is assigned $C$ keys
  – each $K_{d,j}$ where $0 \leq j < C$ corresponds to a key from column $j$ in the scheme matrix
• Device keys must be stored “securely” on each device
Media Key Blocks

- A Media Key Block is a data structure that contains multiple ciphers of the same media key Km under different device keys Kd
Revocation

• To revoke Device B, an MKB is written that has invalid keys in all the positions corresponding to the keys assigned to B.
Threat model I

• Over time, keys *will* be leaked:
  – Reverse engineering
  – “Sloppy” or “evil” licensees

• Solution:
  – Disable compromised keys
  – Prevent “cloned” devices from playing *new* content

• Limitation:
  – As the number of revocations grows, the probability that compliant devices will be disabled increases
Threat model II

• Save/restore attack:
  – Bit-by-bit copy of media contents
  – Delete (e.g. SDMI checkout)
  – Restore media image

• Solution:
  – Dynamic media id (used to compute Kmu) is incremented after every secure delete

• Limitation:
  – Must re-encrypt all title keys with the new Kmu
Tracing

• If a cloned device is “captured,” custom MKBs are created to trace the compromised device keys:
  – For each column, write garbage in the top half and real keys in the bottom half
  – If the player cannot decrypt, write good keys in the top quarter and garbage in the rest
  – Otherwise, continue binary search in “good” section until it is pinned down
  – Proceed to the next column
Call to action

• In the interest of copyright owners, we are making circumvention “inconvenient”

• But we need to make the usage of copyrighted content more convenient for consumers