Content Protection and Copyrights Management over Digital Television Environments

김 형 중
강원대학교 제어계측공학과
khj@kangwon.ac.kr
http://multimedia.kangwon.ac.kr

For Whom?

- Service Providers:
  CA (Conditional Access)
- Content Providers:
  CMP (Content Management and Protection)

CA and Transaction Mechanisms

- *Periodic subscription*: purchasing entitlements, typically valid for one month
- *Order-ahead pay-per-view* (OPPV): pre-paying for a special event
- *Pay-per-view* (PPV) and *impulse pay-per-view* (IPPV): paying close (or very close) to the time of occurrence of the event
- *Near video on demand* (NVOD)

Why CMP ?

- Not only the ease of making copies is at issue, but also the fact that digital copy is as perfect as original and sometimes even better.
- Intellectual property right infringement is a serious threat to content providers.
- Content management and protection is one of the key technology for digital broadcasting, audio and video on demand, and DVD production.
- CMP is just an emerging technology for fighting digital piracy for digital content providers, movie, recording, and broadcasting industries.

Excerpts from Webzine

- The movie industry argues that DTCP should be used more widely than the current specification dictates, including for Internet and over-the-air broadcasts.
- For the machine that's sitting in the catbird seat as far as digital convergence is concerned, MPAA has concerns on two fronts: Internet retransmission and the PC-subsystem interface. At this point, the Internet is the bigger bogeyman.

CMP Examples

- CA for Satellite Broadcasting
- DTCP for DVD
- SDMI for Major Labels

Enabling Technologies

- Authentication
- Content Encryption and Decryption
- Digital Watermarking
- Key Exchange and Management
- Renewability and Revocation
- Tracing Protocols

Three Potential Problems

- How copyrighted and other valuable content can be protected from unauthorized copying?
- How PC and CE suppliers can cost-effectively protect content without inconveniencing authorized users?
- How digital ports (i.e., IEEE 1394) can be practically implemented between PCs and CE devices?

Requirement of CMP Systems

- They should be transparent to the users.
- They should support all potential architectures.
- They should support varying security requirements of content providers.
- They should support any encoding algorithms.
- Security model should be sustainable over decades.
- Requirements on manufacturers should be minimized.

Security Requirements for Contents

- How much security is required for a piece of content?
  - CE devices do not need to fight digital piracy thoroughly and forever.
- Does one security system fit all?
  - One security system may not sufficient for all types of content.
  - One security system can not meet all security requirements forever.

Security over Time

- Security threats continuously evolve.
  - Attack techniques advance linearly with time.
  - New attack techniques develop radically, but only a few of them is disclosed.
- Legacy management is another critical issue.
  - Life span of CE is more than at least 10 years.
  - Life span of security technology is less than 4 years.
  - Hackers may break cryptographic systems far faster than we expected.

Two Important Techniques

- Two important technologies are:
  - Encryption
  - Watermarking
- Encryption-based technologies attempt to protect copyrighted digital content by transforming it into unintelligible format.
- Watermark-based technologies embed data into copyrighted digital content for identification.
- Hybrid technologies combine features from encryption and watermarking technologies.

Encryption-Based CMP System

- Two distinct approaches for developing solutions are:
  - Re-encrypting content
    - The source device encrypts again the content and sends it to the sink device.
    - The sink device decrypts the content and uses it as authorized.
  - Keeping content encrypted
    - The content is encrypted at the origin only. It is not decrypted (during transmission or storage) until it is displayed.
- Hybrid approaches are also possible.

Two Steps in Content Protection

- Content Encryption
  - Symmetric Algorithm is used for fast processing.
  - Different parts are scrambled under different keys.
  - Key is exchanged every few seconds.
- Key Encryption
  - Public-key algorithm is used for security.
  - Public key is not changed.
  - Other algorithms can also be used.

Major Specifications in This Talk

- DTCP: Digital Transmission Content Protection
- IPMP: Intellectual Property Management and Protection

- OPIMA: Open Platform Initiative for Multimedia Access
- SDMI: Secure Digital Music Initiative

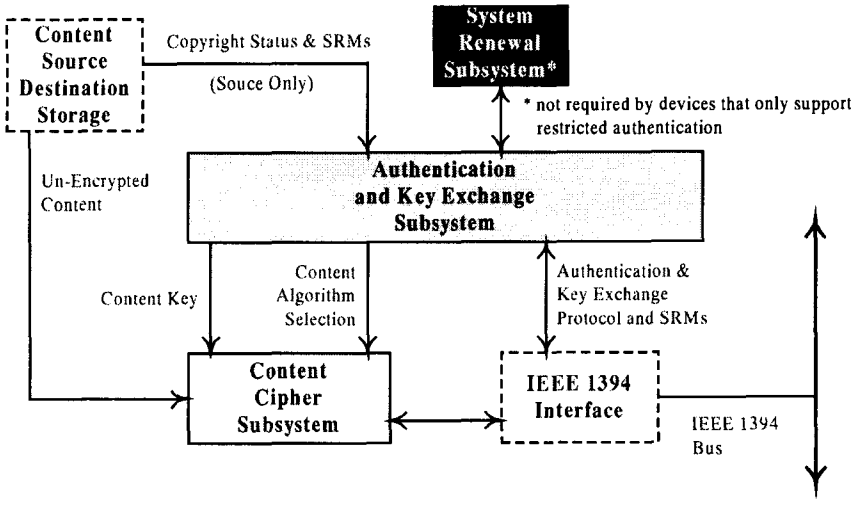
DTCP

- Digital Transmission Content Protection
  - 5C: Hitachi, Intel, Matsushita, Sony, Toshiba
  - Specification Version 1.0 (April 12, 1999)
  - To develop a system that protects the digital transmission of content through both *technical* and *legal* means
- Based on *chip sets* embedded in set-tops
  - Rather than smart cards like XCA (eXtended Conditional Access)

DTCP: Two Deterrents

- Deterrents for Would-Be Digital Pirates
  - If pirates manage to defeat the *technical deterrents*, they would still face *legal action*.
  - This legal requirement is satisfied through the use of technology only available *under license*.
  - Hacking DTCP would violate *intellectual property law*, and subject the hacker to civil litigation.

DTCP Schema



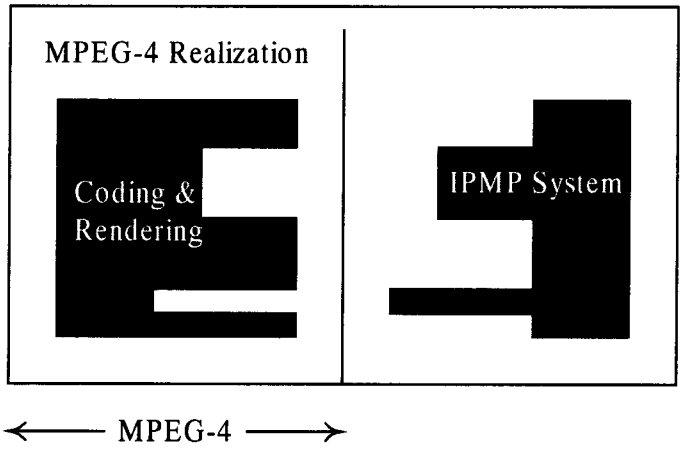
MPEG-2 and Conditional Access

- MPEG-2 system layer makes provision for encryption, permitting program providers to use electronic subscriber addressing and authorization.
- Transport stream header contains a *scrambling control field* to indicate the encryption system in use; and an *adaptation field* for the conveyance of encryption keys and similar codes for the control of access to specific services by individual users.

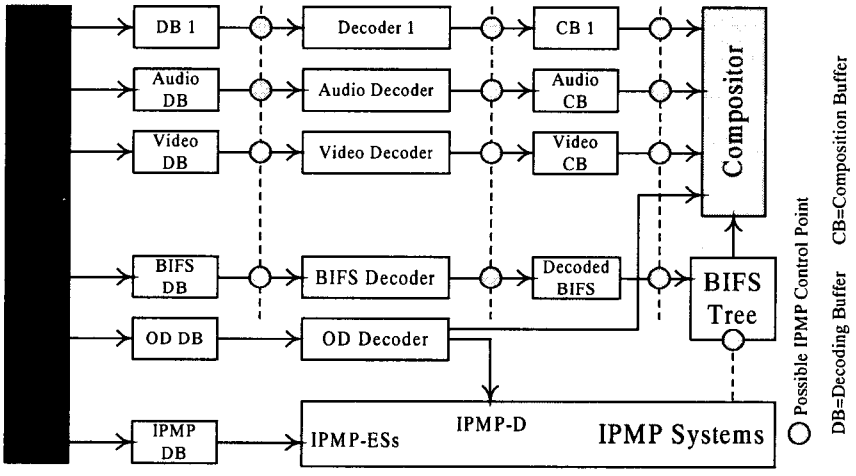
MPEG-4 IPMP

- The IPMP framework consists of a fully standardized IPMP Descriptors (IPMP-Ds) and IPMP Elementary Streams (IPMP-ESs) which are a standardized shell with non-normative content.
- MPEG-4 standardizes IPMP Interface, but not IPMP Systems.
  - This interface consists of IPMP-Ds and IPMP-ESs.
- IPMP is prerequisite for publishing serious and valuable content in digital form (in any open environment).
  - It makes no sense standardizing protection schemes, cryptographic algorithms, and so on.

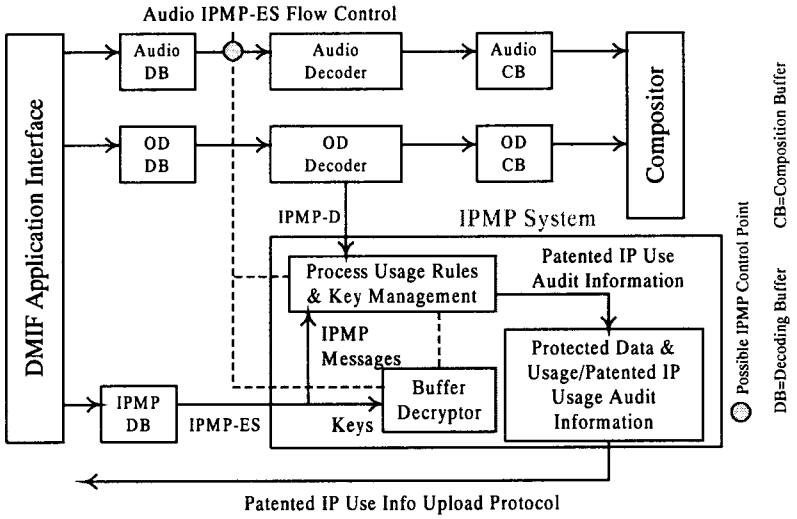
High Level View of IPMP Architecture



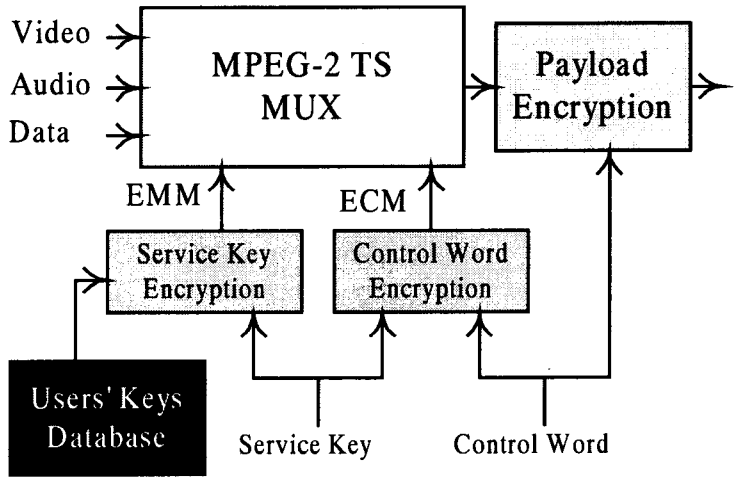
MPEG-4 IPMP Schema



Patent IP Protection in IPMP



ECM and EMM in MPEG-2



ATSC Conditional Access

- A/70 Specification
- *Scrambling*: a method of continuously changing the form a data signal so that without suitable access rights and an electronic descrambling key, the signal is unintelligible
- *Encryption*: a method of processing keys needed for descrambling, so that they can be conveyed to authorized users
- ATSC key is 168-bit long.

ATSC Security Module

- NRSS (National Renewable Security Standard): Part A (Smart Card) and Part B (PCMCIA)
- NRSS-B CA modules shall filter the CAT (CA Table). NRSS-A CA modules may filter the CAT.
- ECM (Entitlement Control Message): data units that mainly carry the key for descrambling the signals
- EMM (Entitlement Management Message): most likely contain information about the status of the subscription itself

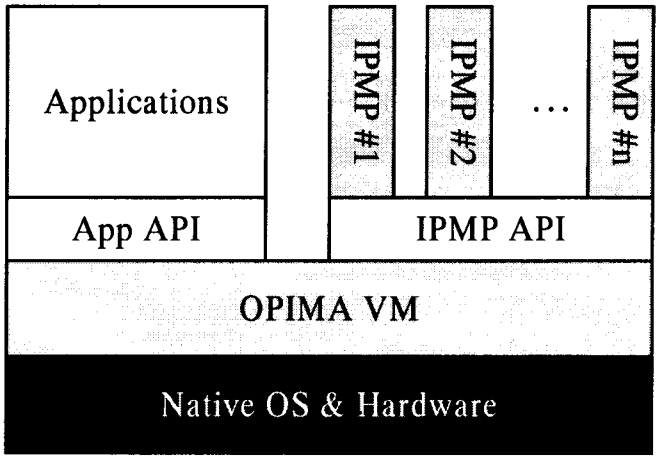
OPIMA

- Open Platform Initiative for Multimedia Access
- OPIMA Specification v. 1.0 (September 1999)
- The Specification presents an architecture and a description of the functions required to implement an OPIMA-compliant system. Furthermore, it presents security protocols and a description of API and functional behaviors that enable interoperability.
- The Specification is independent of device and content.
- Unresolved problems on OPIMA Specification regarding the choice of X.509 or SPKI will be decided in the year 2000.

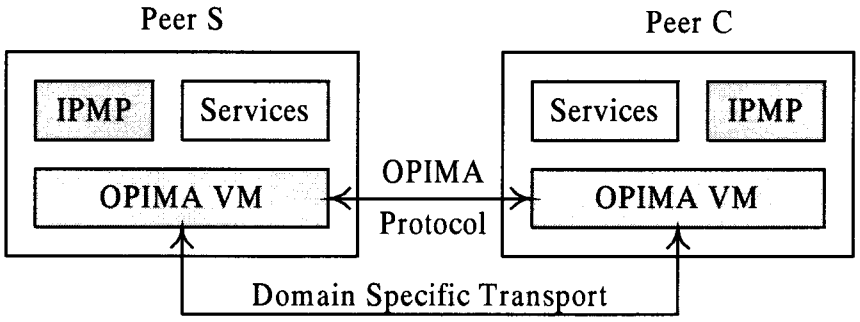
OPIMA Jargon

- Compartment is a class of OPIMA enabled devices that share some common elements in their IPMP interfaces and/or architectural components.
- IPMP System protects and manages intellectual property rights associated with content.
- Credentials is a set of authenticated identifiers certifying the compartment ID and peer ID.
- OPIMA Virtual Machine (OVM) is a group of basic functional elements that implement a secure execution environment for IPMP Systems.
- Rules are statements governing the way a content protected by an IPMP System can be managed.

OPIMA Peer



OPIMA Schema



OPIMA Protocol Example

- An Application requests the OVM to access protected content.
- The OVM requests the OS to establish initial network connection.
- The OPIMA Secure Authenticated Channel is established on top of this connection.
- The required IPMP System is requested and downloaded by the OVM.

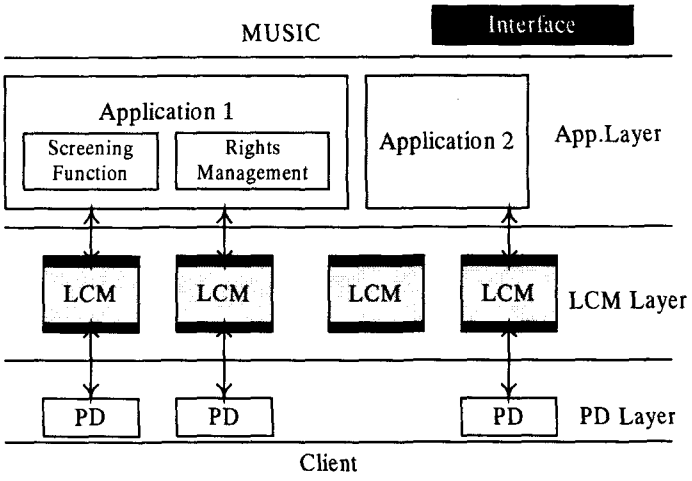
SDMI

- RIAA, RIAJ and IFPI announce SDMI in Dec. 1999.
- Technology companies work together to create an open architecture and specification for digital music security.
- The specification will protect copyrighted music in all existing and emerging digital formats and through all delivery channels.
- The portable devices initially would be allowed to play songs with or without copyright protection, but later versions would be required to block pirated music.
- The next phase will allow the new devices to identify the marking and tell the user to upgrade software to play the recording.

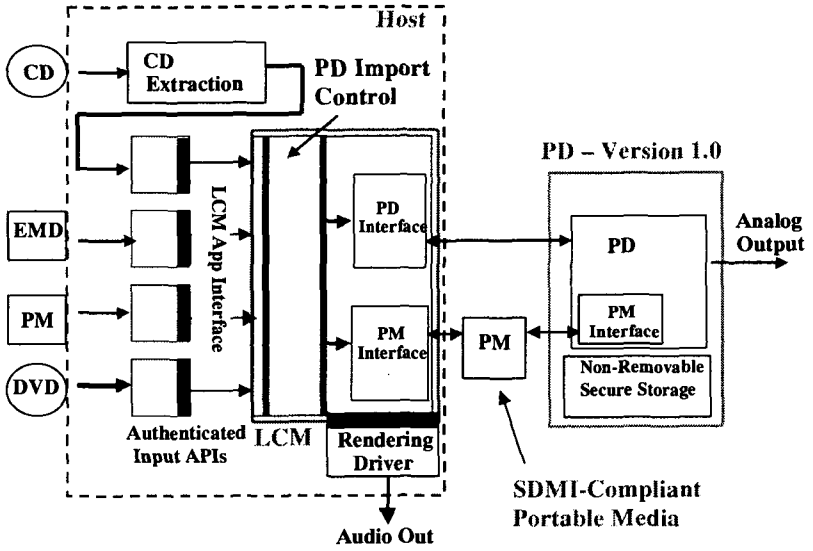
SDMI Jargon

- Licensed Compliant Module (LCM) is an SDMI-compliant module interfacing between SDMI-compliant applications and SDMI-compliant devices, media and components.
- Portable Media (PM) is an SDMI-compliant media that may be used to store SDMI Protected Content.
- Portable Device (PD) is a device that stores on internal or PM SDMI Protected Content received from an LCM residing on a client platform.
- SDMI Protected Content shall be accessed only by SDMI-compliant devices or components within the SDMI domain.

SDMI Schema



SDMI Reference Model



What Can We Do with Watermarks

- Copy Control?
- Content Provider Identification?
- Finger Printing?
- Indexing?

Major Activities

- ISMC for Comprehensive CMP activity
  http://multimedia.kangwon.ac.kr/ismc
- DMC for SDMI Counterpart
  http://www.kdmc.or.kr

- MPEG
  http://drogo.cselt.stet.it/mpeg/
- OPIMA
  http://drogo.cselt.it/leonardo/opima/
- SDMI
  http://www.sdmi.org