Dr Jekyll and Mr Hyde

The Two Faces of MPEG

Avni Rambhia
arambhia@e-vue.com
e-Vue, Inc: www.e-vue.com
Acknowledgement

- Several MPEG-related slides here are taken from Rob Koenen’s presentation to W3C.

- Rob Koenen (rob@intertrust.com)
  - Chairman MPEG Requirements Group
  - President MPEG-4 Industry Forum
Overview

- MPEG
- IPMP
- Protecting Streaming Media
- Issues
- Demos

- Please ask questions as they arise!
What’s MPEG?

- Digital Media compression, delivery & protection

- MPEG-1: Cd-i, (Video CD, VoD, Streaming), ... - 1992

- MPEG-2: ... + TV, HDTV - 1994

- MPEG-4: Coding of Audiovisual Objects - 1998 (V.1), 1999 (V.2), extension work ongoing

- MPEG-7: Description of Multimedia Content - 2001

MPEG-4: Multimedia Streaming

- Media
  - Synthetic, Natural, Animated
  - Audio, Video, Image, Graphics, Meshes, Text
  - 2D, 3D

- Interactivity
  - Client/Server, Programmable Multimedia

- Universal Access and Network Quality
  - Any transport protocol, wide bandwidth range

- Maximal Compression
Bandwidth Perspective

- **Wireless**: 5 Kbps, 28 Kbps, 56 Kbps, 500 Kbps
- **Dial-Up**: 1.0 Mbps, 1.5 Mbps, 4.0 Mbps
- **DSL, Cable Modem**: 6.0 – 8.0 Mbps (DVD)
- **Digital Set-Top**: 20.0 Mbps
- **3G Wireless**: 20.0 Mbps
- **HDTV**: MPEG-4/2

- **Digital Set-Top**: MPEG-1
- **MPEG-4**: “VHS” ~500 Kbps
- **MPEG-4/2**: “DVD” ~1.0 Mbps

---

- **RN, MSFT, QT**: MPEG-1
The Big Picture

Individual Streams from MPEG-4 Servers

Audio 1
Audio 2
Video 1
Video 2
Image 1
Initial Scene Description

IPMP/DRM

Network

MPEG-4 Player

Object 1: Audio 2
Object 2: Video 1
Object 3: Image 1

Final Scene Description

Object 4: IPMP/DRM

Decoder

Composer

Renderer

Scene Playback

User Interactivity
Streaming Media Delivery

- MPEG-4 is a wonderful media compression and delivery framework.
- For content providers, quality isn’t enough.
- You need security too!
- Infrastructure monetization is essential as well.

- What’s the big deal with piracy?
Piracy – The menace(?) worsens

- Mechanical: One Generation
- Analog: Limited Generation, Low Speed, Physical Transfer
- Digital: Unlimited Generation........
Digital Multimedia Piracy

- Leaves original behind –
  - Owner doesn’t lose, supplier does (unlike physical media)
- Copies are perfect – unlimited generations
- Possession does not imply right to use
  - Simultaneous users
- Acquisition is cheap and easy
  - Infrastructure is almost free (www, open-source)
  - Recording devices are cheap
  - Easy access (Napster, iMesh, insiderZ)
  - High compression, great quality
    - MP3, DivX: Thanks, MPEG 😊
DRM/IPMP

- Digital Rights Management
- MPEG-speak: Intellectual Property Management and Protection
- The last frontier for streaming multimedia
  - Compression and bandwidth are achievable
What is IPMP?

- Your Intellectual Property is anything whose use owes you some form of compensation. This could be the media, or it could be technology the media uses.
- Managing IP involves storage and serving, appropriate authorization of use and correct billing and tracking.
- Protection prevents unauthorized use or misuse of the IP, and eases legitimate use.
IPMP Process Overview

PUBLISHER
- Management
- Protection

SERVER
- IPMP System Update, Usage, Audit

PLAYER
- Rights
- Application
- IPMP System

USER
- $
Encryption Issues

- Percentage of data encrypted
  - Security v/s client power trade-offs
  - ‘Smart’ media-specific encryption of critical data
- Frequency of key change
  - Broadcast v/s Multicast
  - Security v/s overhead
  - Mobile agent-based? Multi-tier encryption?
- Error-resilient encryption
  - Keep bitstream compliance to use error-resilience schemes
  - Encrypt between resync markers
  - Do not create false start codes or resync markers
  - Redundant encryption?
Convergence Issues

- Using scalable streams, the same media can be served over different bandwidths
  - Different bandwidths cater to different devices
  - Different devices use different (standardized) IPMP schemes
- Most ‘P’ schemes differ only in configuration data format and protocol.
  - Multiple IPMP data streams are needed
- ‘M’ schemes could be handled by different server types.
Rights Definition

- Consistent usage definition
  - What does ‘play’ mean?
- One-size-fits-all scheme
- Parser complexity v/s scheme flexibility
- Compression
  - ODRL or XrML files are easily 2K in size
  - Very easily compressible
  - MPEG-4 precedents in binary representation of VRML.
- Semantic overload?
Server Issues – Media, Rights, Sys

- Access control is very important
  - Bandwidth may be under IPMP
- Key delivery and renewal is a huge scalability issue
- Synchronization of media and key information
  - They could come from separate servers!
- User trauma recovery v/s fraud
- Dynamic revocation of certificates in case of compromise
Player Issues: Security

- The client is always an adversary
- On open environments, secure execution between application and third party IPMP tools
- Sending a key and algorithm across an interface is as secure as passing cleartext data through an interface
- Insertion of fake protection (for data tapping, e.g.) should be detectable
- It all comes down to ‘trust’
Desirables

- Seamless integration between the IPMP System and Terminal
- Operation of several different IPMP Systems in parallel

- The above two are often conflicting requirements!
MPEG is essentially a terminal standard
MPEG’s goal is interoperability

There are two kinds of interoperability
- From the manufacturer’s point of view: clear interfaces between different components
- From the consumer’s point of view: content from any source will play on players from any manufacturer

MPEG cares about consumer interoperability.
What interoperability boils down to

- A Rights Language is nice, but not nearly enough
- **Trust** (trust, trust, ... etc.)
  - A content provider trusting the IPMP System
  - An IPMP System trusting the player
  - A Player trusting the Platform
  - Content trusting the Player, the Platform
- Trust is not (just) technical
  - Just a PKI infrastructure will not get you there
  - You need tamper resistant implementations (HW, SW)
  - Who will do due diligence on a player?
  - Who will check the platform?
  - Etc.
- A **trust infrastructure** is required
IPMP and MPEG

Historically
- content identification has been standardized
- IPMP ‘hooks’ have been defined

IPMP implementations have been proprietary
- Some white box IPMP systems were designed for specific application spaces (CA, DVB)

This led to one IPMP System per player

It won’t work anymore
MPEG-2 IPMP

- **Identification**: copyright descriptor = identifier + number
  - Identifier refers to Registration Authority (such as ISBN)
  - Number is unique ID handed out by authority
  - MPEG does not technically enforce integrity of this information
    - MPEG has no other ways to enforce this
    - Removal or alteration is, however, prohibited by international treaties and legislation.

- **Protection**:
  - Encryption messages
  - Provisions for signaling the presence of encryption and the type of Conditional Access system used.
  - No standard DRM

Internationally recognized ID systems

Hook for proprietary protection systems
MPEG-4 version 1 IPMP

- **Identification**: IP dataset
  - content type selected? (y/n)
  - registration authority ~ registration number ~ title ~ supplementary information ~ references to IP info
  - Can be attached at any level of granularity

- **Protection**: standard interfaces to proprietary IPMP systems
  - In 1997 broad consensus NOT to specify IPMP System
    - One size does not fit all (Cost-Benefit)
    - Fear of laundry of high value content through low protection devices
  - Tight integration of ‘hooks’ with MPEG-4 Systems layer
    - Special Descriptors and Stream Type for IPMP information
    - Special Registration Authority for registering IPMP Systems
    - Architecture allows management next to protection
    - (you can read this at home)

- **At any level of granularity!**
Extending MPEG-4 IPMP Architecture

- Who wants 5+ different portable music players?
  - SDMI will not solve the problem

- More interoperability is required!

- Second MPEG-4 IPMP Call for Proposals in July 2000
  - High level, user-oriented requirements, e.g.
    - Easy to use, on-line and off-line
    - Play content from different sources without changing hardware
    - Move content around on your devices, lend it out, subscribe etc.
    - Protecting privacy
    - Etc.
  - 13 Submissions received in October 2000
MPEG-4 IPMP Extensions: Status

- Goals translated into:
  - Allow protected content played on terminals having IPMP systems supplied by different vendors;
  - Allow IPMP tools supplied by different vendors protecting the same piece of content in a given terminal.

- Current approach:
  - Declarative representation of IPMP tools
  - IPMP Tool-to-Terminal communication protocols
  - Terminal identification verification and credential exchange
Bottomline for Player

- Interoperability
- Ease of Use
- Cost efficiency
- Computation efficiency
- Secure
- Reliable
- Renewable
- Upgradeable
- Transferrability
Summary: The ‘Keys’ to Success

- M&P cost is a reasonable fraction of IP cost
  - File size cost
    - 20KB license and data for a 5KB media file
  - Player/device cost
    - $10K dongle for $5 media, or 200KB protection dlls for 100KB ActiveX control
  - Monetary cost
    - 80% of your long distance bill is tracking cost
- Computing resources
  - Memory, speed, chips
- Time and accessibility
Summary: The ‘Keys’ to Success -2

- Guaranteed access and delivery
  - QoS over jittery bandwidth
  - Error resilience
  - Scalable, reliable server infrastructure
  - Offline availability? Simultaneous use ramifications
  - Subscription models help?

- Portability of content for user, security for content providers
  - No unauthorized transfer and/or use
  - Easy authorized transfer and use
  - Cell-phone tie? Smart card? Big Brother?

- Flexibility – different media and users have different protection needs.
Summary - Open Issues

- Error Resilience
- Scalability
- Key Management
- Synchronization
- Trust
Demos, Questions?

- MPEG-4 video protected, using Access Ticket Systems protection and e-Vue MPEG-4 technology

- Questions?