Digital Rights Management in the Internet

Jason But
jbut@swin.edu.au

Internet Applications

- Email
  - Text/data transfer between individuals (one-to-one distribution of content)

- WWW
  - Content publication (one-to-many distribution of content)

- Interactive
  - Conferencing (private peer-to-peer communications)
  - Games (Data typically not subject to theft)
Profitability of Applications

- Internet Applications involve costs
  - Content development costs
  - Artistic (Intellectual) Property
  - Service Provision Costs
- Services will only remain viable if costs are recouped and a profit is made

Intellectual Property

- Content intellectually belongs to artist who created it
- Can be bought and sold (Copyright ownership)
  - Copyright ownership can be viewed as an investment
  - Return is required
  - Typically involves payment by the consumer for the privilege of accessing the content
Copyright – Generating Returns

- Traditional Methods of Generating Returns
  - Public broadcast paid for by broadcaster via advertisers
  - Pay-per-access paid for by viewers and potentially advertisers
  - Purchase – CD or DVD type purchase involves purchase of right to access content, not to own it

- Potential Methods of Generating Returns on Digital Availability
  - Pay-per-access by customers
  - Public availability paid for by advertisements on web sites

Copyright Protection

- Digital copies are easy to make
- Theft is easy – witness Napster
- Protection against digital theft is imperative
  - If protection is not offered, Copyright owners will not make content available online and these types of applications will not exist
Copyright Protection

• Passive
  • Watermarking (Message Hiding)
  • Dependent on content type
  • Used to help prosecute after theft has occurred

• Active
  • Encryption (Message Scrambling)
  • Theft of content occurs but decryption is hard
  • Key Management becomes an issue
  • Used to discourage theft through required outlay

Digital Rights Management

• Not just copy protection
  • Collection of money for right to access content
  • Determination of license provisions
  • Delivery of license
  • Enforcement of license provisions
  • Copy Protection
  • Watermarking
  • Distribution of monies to content/service providers

• Framework above underlying delivery applications
Traditional Content Delivery Model

Cached Content Delivery Model
Cached Delivery Model with DRM

Encryption in Application Space

- Basic encryption of content is OK for simple store-and-forward type data
  - Stored at cache in encrypted form
  - Forwarded to authorised used for decryption and usage
- What about complex data access?
  - Streaming Audio/Video
  - Access to databases
  - Interactive Applications
Encryption in Application Space

- Caches must be smart, provide more functionality than just store-and-forward
  - Distributed Server Architectures
- Encryption becomes integral part of caching problem
  - Content must be protected
  - Caches must still provide complex functionality.
- Caching digital content has implications for how Copyright protection is done

Encryption of Cached Content

- Encrypted Content must be stored on caches
  - Real-time encryption of data has scalability issues
  - Caches vulnerable to attack for theft purposes
- Cache implementations will be provided by numerous vendors
  - Not all will agree to implement a complex encryption algorithm
  - Incompatibilities between implementations
  - Selection of implementation by a content/service provider locks them into a monopoly
  - Less competition amongst platform providers => higher costs
Encryption of Cached Content

- Selected cipher must be compatible with all caching implementations
  - Including those with no encryption capabilities
  - No problem for store-and-forward, an encrypted file is treated the same as a plaintext file
  - Advanced functionality, encrypt data but leave metadata as plaintext so existing products can continue to deliver services

- Examples
  - Streaming Audio/Video – Distributed servers should still provide advanced playback functionality
  - Database accesses – Queries into encrypted data without knowing the contents of that data must be supported

Summary

- Internet will continue to grow, supporting new applications
- Digital Rights Management must be implemented on applications that seek to be profitable
- Copy protection is an aspect of Digital Rights Management
- Caching entails multiple digital copies of content are littered throughout the network
- Copy protection schemes must be compatible with existing caching schemes
  - If caching involves advanced functionality, then this must be taken into account
- Copy protection, particularly encryption and watermarking schemes must be implemented with compatibility with existing systems in mind