Implementing Encrypted Streaming Video in a Distributed Server Environment

Jason But

Outline

- Online Streaming Video
- Higher Quality Streaming Video
  - Caching
  - Commercial Content
- Copyright Concerns
- Protecting Copyright
  - Watermarking
  - Encryption
- Requirements for Ciphers with Streaming Video

Internet Streaming Video

- A commercially successful service must compete with TV/DVD Hire
  - Attractive content
  - Higher quality – increased encoded video bitrate
- Network Problems
  - Sensitive to Network jitter and delay variation
  - Minimised by:
    - Decreasing hop count to streaming server
    - Increasing playback buffer at client

Higher Quality Video
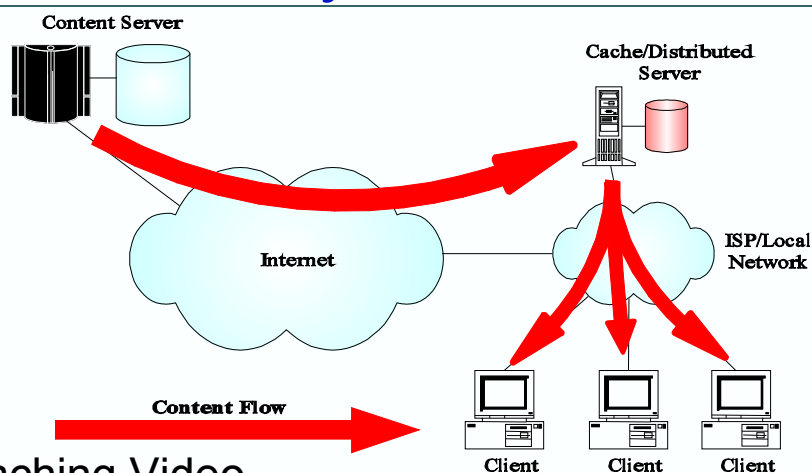
- Caching Video
  - Decreases hop count to client
  - Reduces core network traffic and user response time
  - Caches must implement advanced playback functionality (eg. pause, indexed playback, high-speed playback modes)

Copyright Concerns

- Copyright is important
  - A viable service will be one that offers commercially successful content
  - Content will only be made available if copyright can be protected
- Watermarking
  - Passive Protection
  - Assists in prosecution *after* theft has occurred
- Encryption
  - Active Protection
  - Discourages theft in the first place
  - Does not stop distribution of pirated content after decryption
- Need both types of protection

Protecting Streaming Video

- Watermarking is transparent
  - Watermarked digital video can be streamed by all video content streaming systems
- Encryption must be compatible with existing and future streaming video systems
  - Cipher is developed by experts in ciphers and not by streaming video developers
  - Streaming video development does not need to consider encryption
  - Increased competition between streaming video developers

Encrypted Streaming Video

- To do this the cipher must:
  - Allow location of key reference points within the encrypted bitstream (allowing indexed and high-speed playback modes)
  - Correctly resynchronise in all supported playback modes
  - Be independent of the video decoder
  - Be computationally efficient – supporting software video decoding
- No current video ciphers support all of these properties

Conclusions

- Copyright protection is imperative in providing a commercial streaming video service
- Achieved through both Watermarking and encryption
- Ciphers must
  - Be independent of streaming video (server and client) implementation
  - Support all digital playback modes