Content and License Roaming for eHome DRM Applications

Bin B. Zhu and Shipeng Li

Microsoft Research Asia
{binzhu,spli}@microsoft.com

Outline

- Introduction: DRM system
- Requirements in eHome applications
- Optimus project for eHome
- Optimus DRM solution
- Conclusion
- References

Introduction – DRM System

- Digital Rights Management (DRM) system:
  - Provide persistent protection & rights management throughout the entire life of a digital asset
  - Content and rights (i.e., license) objects are separated
  - Content encrypted with symmetric encryption (& may be watermarked)
  - Rights expressed in rights expression language (XrML, ODRL, etc.)
  - Licenses individualized with public key encryption and certificates & bound to device/storage hardware

Requirements in eHome Applications

- Features in eHome applications:
  - Same content may be played by devices with a variety of capabilities and display characteristics
  - Content may be streamed in protected format to devices through home networks of different characteristics and varying bandwidths
  - Protected content should be easily shared and played with different devices (PC, PocketPC, SmartPhone, portable players, remote display, etc.)
- DRM for eHome should provide easy sharing of content & rights among eHome devices yet troublesome if not at all in sharing with other people

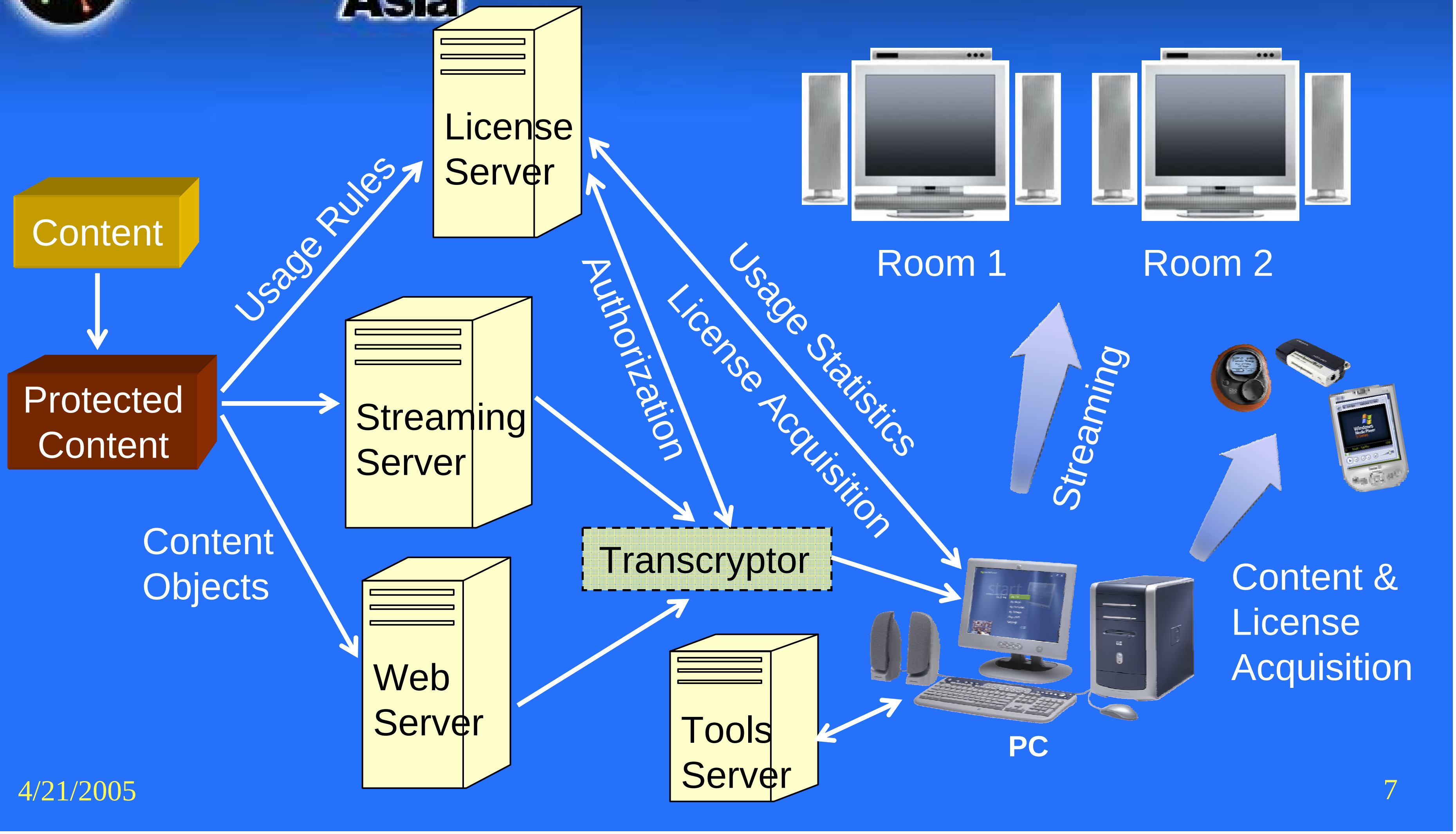
Limitations of Traditional Systems

- eHome devices have a variety of capabilities (display, storage, processing power, etc.)
- A traditional multimedia system is not scalable or scalably encrypted, and is difficult for content sharing
  - Same content is compressed & encrypted to multiple copies, each tailored to fit a specific device/network
  - Different copies protected with different keys, and difficult to share among eHome devices
  - Inefficient to stream protected content to different capable devices
- Licenses tied to devices and difficult to share among eHome devices.

Optimus Project

- A research project for eHome applications
  - Based on SMART [1] scalable system
    - Content consists of a base stream and 0 to many enhancement streams
    - Base stream is non-scalably compressed and enhancement streams are scalably compressed.
    - Bitrate/quality/frame size/frame rate/complexity scalable
    - Layered, block-level, or fine granularity scalability
  - Enhanced ASF format [2] and Windows media system [3] to support scalable A/V formats & systems
  - Same protected content shared among devices
    - Metadata for truncation points & R-D optimal truncation.
    - Directly reshaping protected data to best-fit devices.
    - Streaming base & enhancement streams concurrently for devices to select best-fit combination of streams
  - Smooth roaming among different eHome networks (e.g. wired Ethernet to wireless)
  - Provides easy and near transparent content and license roaming among eHome devices
  - Converts other A/V format media to SMART on the fly through trusted nodes or clients/modules

DRM System for Optimus



DRM System for Optimus (cont.)

- Different DRM tools are supported & downloaded from DRM a tool server for flexibility & extensibility.
- Tools must be registered, authorized, & authenticated by a centralized authentication server before uploaded to tools server
- Client device is authenticated and verified to meet minimum security requirement before a tool installed to it
- The DRM system in the presentation is described for Optimus but also applicable to generic digital content and multimedia formats/systems

Transcryptor

- Converts protected A/V content of other formats to supported formats
- Optional – used only if content is not in right formats
- Executed by a trusted party
  - Trusted node/server
  - Trusted DRM module at client such as user’s PC.
- Authorized by license server per content
- Authenticated to license server & checking possible security compromise before authorized
- Secrets bound to hardware & delivered through initialization (may be combined with client’s DRM individualization [4] during setup)

DRM Encryption Requirements

- Fast encryption & low complexity decryption
  - For streaming applications, transcryptor may need to re-encrypt on the fly
  - Portable devices may not have enough processing power
- Preserve fine enough scalable granularity in encrypted streams
  - Enable reshaping directly in ciphertext for devices with different capabilities
  - Enable directly streaming encrypted content to multiple devices via home networks with varying bandwidths
- Robust to packet loss and bit errors in transmission (such as streaming through home wireless network)

Default Encryption Tool for Optimus

- Content-agnostic: applicable to different content types
- Content encrypted with a modified RC4 [5] or AES, license encrypted with RSA.
- Each stream or payload can be selected to be encrypted or non-encrypted.
- Data in each payload/subpayload is independently encrypted
- Encrypted streams can be truncated or reshaped at subpayload granularity. Finer granularity protection such as [6] can also supported (with a different encryption tool).
- Base stream may be unencrypted or weakly encrypted for targeted low price eHome devices. Security is strengthened with strong encryption of enhancement streams
- Multi-layer and multi-access protection described in [7-8] are supported
- Optional metadata helps to truncate an encrypted content directly and content-agnostically to best fit an eHome device

Content Sharing Among Devices

- Enhancement data is partitioned into multiple streams so fine that stream-level truncation is used for typical eHome devices
- Incremental download is supported
  - stream-level truncation reduces complexity to manage content synchronization for incremental download
- Each device's characteristics are registered at the master device (typically a PC). A best-fit representation of the content is automatically reshaped and transferred from master or another device network-connected to master to the targeted device with minimized human interfaces

Content Streaming

Microsoft Research Asia

- Encrypted content can be streamed from a master device (a PC such as Media Center) to remote device(s) to play
- Base and multiple enhancement streams are streamed through home networks & a remote device can select best-fit data to decrypt and decode.
- Master reshapes scalable streams according to varying bandwidth
- Content streaming can roam from one eHome network to another (such as from wired Ethernet to wireless).
- Network packaging tries to align with subpayload boundary if possible.
- In streaming applications, a remote device does not store protected content.
- All received data is pushed from network layer to application layer to process. For default encryption tool, if partial data is lost, the whole subpayload is dropped by application.

License Management

Microsoft Research Asia

- License is cryptographically bound to each device/storage media
- DRM module for each device is individualized during setup
- License classified into two types: full and transient
  - Full license is the conventional license
  - Transient license is a restrictive license valid for a short time (specified by content publisher)
- Typical management of full licenses (acquisition, revocation, restoration, etc.) is the same as Windows Media DRM [4]
- A master device (master) such as PC behaves as eHome license server & issues transient licenses to other devices (clients)
- An client may contain both full and transient licenses for different content
- A license for a remote device in streaming applications is only valid for the current streaming session.

License Roaming

- Transfer/issuing rules are specified by content publisher and contained in the full license stored at master such as:
  - Transferable or not
  - Can transient licenses be issued? What mode? (see next)
  - How long a transient license is valid in default and extensive modes
  - How many client devices can be issued to in both modes
- Full license can be transferred from one device to another to use remaining rights. Once transferred, old device can no longer consume the content or issuing transient licenses
- Master issues transient licenses to one or multiple clients according to the rules set in the full license
  - Each master can issue transient licenses until reached a max. # of clients
  - Each client must be registered before master can issue transient licenses to it
  - Each client meet minimum security requirements
  - A client can be released from registered clients when connected to master which invalidates all transient licenses
  - A client can also be released from registered clients by claiming lost
- Each client can have at most one master
  - If a client is reused with another master, it has to un-register with the old master
- Each master must meet minimum security requirements

License Roaming (cont.)

- Released registration due to loss is remembered by master for a certain period of time:
  - Lost devices cannot re-registered with a master for a certain period of time unless no device is registered after lost
  - Used to prevent getting around of max # supported clients by claiming lost.
- Master and client authenticate to each other before a transient license is issued.
- A sync. list on each client is used to monitor and manage transient licenses
  - transient licenses on the sync list renewed automatically when device is connected to master
  - Warning for expiring transient licenses and prompt for renewing
- For certain rights such as playing n times, an default or manual splitting is needed in issuing transient license
  - A metering variable indicates allocated rights to clients
  - The variable is adjusted at each issuing or a transient license release unused rights
  - The variable is checked in issuing transient licenses or consuming protected content
- Master may issue transient licenses in the extensive mode (valid for a longer period of time for long time away from master such as traveling, etc.)
  - A list of full licenses issued with extensive transient licenses is stored securely in master
  - A license is removed from the list if the period expires, the client reconnected to master, or lost.
  - Master cannot transfer/issue license or play content when its license is in the list

Statistics Collection

- Certain statistics is collected by master from all registered devices & transferred to a server, such as:
  - How many transient licenses issues per content?
  - How many devices played a content? How many times? When? Used to estimate
    - How well a content is received
    - How many users per eHome & possible price adjustment in the future

Some Key Modules

- Secure Clock & Synchronization
  - Each device should have a tamper-proof clock mechanism (at least rollback-proof for clients)
  - Clock is synchronized/adjusted against master device’s clock
- Secure storage for metering data etc.
- Tamper resistance DRM module at client
- These modules are either reused from or implemented after those of Windows Media DRM [4].

Conclusion

- A secure DRM system for Optimus has been described
- The system facilitates easy roaming of protected content and licenses among eHome devices
- Default encryption tool supports content-agnostic protection with subpayload scalable granularity
- The system is flexible and extensible to support new protection mechanisms/tools
- The DRM system is also applicable for rights protection and management of generic digital assets.

References

1. F. Wu, H. Sun, G. Shen, S. Li, Y.-Q. Zhang, B. Lin, and M.-C. Lee, “SMART: An Efficient, Scalable, and Robust Streaming Video System,” EURASIP J. Applied Signal Processing, vol. 2004:2 pp. 192-206, 2004.
2. *Advanced Systems Format (ASF) Specification*, http://www.microsoft.com/windows/windowsmedia/format/asfspec.aspx
3. *Windows Media*, http://www.microsoft.com/windows/windowsmedia/default.aspx
4. *Windows Media Digital Rights Management (DRM)*, http://www.microsoft.com/windows/windowsmedia/drm/default.aspx
5. M. H. Jakubowski and R. Venkatesan, “The Chain & Sum Primitive and Its Applications to MACs and Stream Ciphers,” *EUROCRYPT’98*, pp. 281 – 293, 1998.
6. C. Yuan, B. B. Zhu, Y. Wang, S. Li, and Y. Zhong, “Efficient and Fully Scalable Encryption for MPEG-4 FGS,” *IEEE Int. Symp. Circuits and Systems*, Bangkok, Thailand, vol. 2, pp. 620 – 623, May, 2003.
7. C. Yuan, B. B. Zhu, M. Su, X. Wang, S. Li, and Y. Zhong, “Layered Access Control for MPEG-4 FGS Video,” *IEEE Int. Conf. Image Processing*, Barcelona, Spain, vol. 1, pp. 517 – 520, Sept. 2003.
8. B. B. Zhu, M. Feng, and S. Li, “An Efficient Key Scheme for Layered Access Control of MPEG-4 FGS Video,” *IEEE Int. Conf. on Multimedia and Expo*, Taiwan, June 27-30, 2004.