Digital Rights Management in a 3G Mobile Phone and Beyond
Table of Contents

- Introduction
- DRM Concepts and strategies
- Our DRM system
  - DRM Manager
  - Trusted Application Agents
  - Security Agent
  - DRM Credential
- Security issues
- Family Domain
- Example Use Case
- Conclusion
Digital contents is lucrative

- Shared amongst multiple class of devices (3G Phone, PC, Car stereo)
- Problem – Contents can be shared at no cost. (Napster, Morpheus, Gnutella)
- Entertainment industry losing money

Solution

- Digital Rights Management (DRM)
- Content provider and consumers benefit
DRM concepts and strategies
- Overview of Trusted DRM System

License File
- Metadata
- Rules
- Encrypted Key
- Hash
- Signature

Protected Content File

Encrypted Content

Trusted DRM System

DRM Services

Rendering Software

Output Content
Secure Digital Music Initiative (SDMI) provided an incomplete solution
- Not just rendering content, but stream, copy, or backup needed
- Payment mechanisms

Keitaide-Music System
- Secure system to deliver music to mobile phones
- Trusted memory card for protection

Motion Pictures Expert Group (MPEG)
- DRM Hooks, XrML (rights expression)
- Many more different and incompatible solutions
  - Focus is on common essential architectural elements
DRM concepts and strategies
- Open Mobile Alliance DRM (OMA)

- Open Mobile Alliance (OMA)
  - Develops **open standards** for the mobile phone industry
  - Version1 DRM specification

- Open Mobile Alliance DRM
  - Goal
    - Devise a **consumer-friendly** DRM standard

  “Content files can be distributed to other devices, but that licenses to use this content must be obtained from a server called the right issuer”

- “**Family Domain**” approach will be shown later
  - Distributed contents to all devices owned by a consumer
  - No need to acquire a new license for each transfer
**OUR DRM SYSTEM**
- Interface for DRM

- Number of ways to use DRM
  - Two approaches noted in Schneck’s paper
    - Replace the I/O elements of OS with new modules
    - Hyperadvisor

- Our Approach
  - **OS is extended** to support DRM functionality
  - Access these extended system through API
    - A header indicates if that is protected
    - If file is protected -> call extended API
  - These extensions - “privileged mode”
  - Applications - “user mode”

Figure 2: Generic OS extended with DRM and security capabilities
OUR DRM SYSTEM  
- DRM manager

- Authenticate Licenses and Content
  - Verify Cryptographic hash of the license file
  - Cryptographically linked to content
    - Hash table
  - Digital signature
    - With the help of Security Agents,
    - Public key trustworthiness also checked

- Enforce Rights
  - **Actions** can be associated with three types of **rights**
    - Render rights, Transport rights, Derivative work rights
  - Rights to an action are assigned to a device
    - Use device’s credentials (key/certificate manager)
  - Perform additional event for an action
    - Secure database

- Decrypt Content
  - **Decrypt** the content using key
  - Route it to a trusted application agent, not top-level application
OUR DRM SYSTEM
- DRM manager

Top-Level Application Steps
1. Authenticate license and content
2. Use credentials and request an action (e.g., play, copy)
3. Control the action

Trusted DRM Manager
- Authenticate
- Enforce Rules
- Decrypt
- Trusted Agent
- Secure Database
OUR DRM SYSTEM
- Trusted Application Agents

- **Actually** access and manipulate decrypted content
  - Privileged, and trusted
- **Rendering Agents**
  - **Render** DRM-protected content
  - Interact with top-level GUI
- **Transport Agents**
  - **Move** content from one location to another
  - Establish a Secure Authenticated Channel (SAC)
- **Derivative Work Agents**
  - **Extract and transform** protected content or license into a different form
  - **Installation** of DRM-protected software or data
    - Vulnerable to copying
    - **Access-controlled file system** maintained by security agents
OUR DRM SYSTEM
- Trusted Application Agents

Top-Level Application Steps
1. Use a derivative work agent to decrypt and load a new ringtone
2. Use a transport agent to link phone to headphones
3. Use a rendering agent to play the ringtone

Trusted Application Agents
- Installer
- Secure Link
- Ringtone Player

Audio
Decrypted Ringtone
Access-Controlled Files
DRM System – Security Agents

- Handle the security-related functions
  - Memory and File management
  - Cryptographic operations
  - Key/Certificate management
- Memory and File management
  - Access-controlled file system
    - To store decrypted content
    - Only trusted agents will be allowed to access the content
  - Memory separation system
    - To ensure that if a trusted operation is running, untrusted operations can’t eavesdrop on the memory
  - Secure memory system
    - Prevent critical data (private key) from leaking out of the system
    - If suspicious events occurs, the memory is immediately cleared
Cryptographic operations
- Using symmetric key algorithm (ex. AES)
- License is bound to the content file using a Hash of the content file (ex. SHA-1)
- Public key for content-key encryption, signature generation and verification etc (ex. RSA, ECC)

Key/certificate Manager
- Securely handle a database of the phone’s credentials
  - Keys, Certificates, IDs
- Parsing and verifying the appropriate certificates
<table>
<thead>
<tr>
<th>Operation</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash of a license (5KByte)</td>
<td>SHA1: 3 ms</td>
</tr>
<tr>
<td>Verify license signature</td>
<td>RSA(1): 100 ms</td>
</tr>
<tr>
<td></td>
<td>ECC(2): 150 ms</td>
</tr>
<tr>
<td>Decrypt content key</td>
<td>RSA(1): 1,800 ms</td>
</tr>
<tr>
<td></td>
<td>ECC(2): 90 ms</td>
</tr>
<tr>
<td>Decrypt content (2 Kbyte)</td>
<td>AES(3): 1.6 ms</td>
</tr>
</tbody>
</table>

(1) 1024-bit RSA with CRT  (2) WTLS Curve 3  (3) 128-bit key
DRM System – DRM Credentials

- Serial and Model numbers
  - Serial Numbers
    - Unchangeable number that identifies the phone
  - Model Numbers
    - Number that identifies HW and SW version
- Root Key
  - Check the authenticity and integrity of the credentials
- Private Keys and Certificates
  - KuPri and UniCert
    - Used for establishing Secure Authenticated Channel(SAC) to a phone
  - KdPri and DRMCert
    - Used for assigning content to a device
Security Issues

- Licenses
  - Need to verify integrity and authenticity of licenses
    - Value that links license to content
    - Rights allowed
    - Decryption means
    - Signature
  - Integrity and Authenticity
    - Public Key Infrastructure
    - Private and Symmetric keys must be kept secret
Security Issues

- **Rights Enforcement**
  - DRM manager should enforce rights responsibly
  - Parse license file and process rights expressions
    - Recognize version of license file

- **Content Protection**
  - Rendering software should be trusted to not leak or copy the decrypted content
    - Obtain decryption key CEK
    - Use KdPri to decrypt CEK
    - Establish SAC using CEK and UnitCert and KuPri if necessary

- **Privacy Issues**
  - User information and identity must not be disclosed
    - Without explicit consent of end user
Family Domain

- The consumers don’t want to be locked to one particular device
- Consumer decides which devices belong to his domain
  - Portable devices are assigned to a particular domain by registering with the DA (Domain Authority)
- A trusted server, DA installs common DRM private key in all these devices
  - Domain private key
- A device needs to register with a DA once, and could access to all the content in a domain with domain private key
Domain Authority could tie the domain to user’s private information (like credit card number) to prevent abuse of sharing family domain passwords with others.
Example Use Case

Green Key: KdPri
Blue Key: KuPri
Yellow Key: KdPub
Conclusion

- DRM framework is proposed for a mobile phone environment
  - Also applicable to other devices
    - PDA, tablet PC, automobile, set-top box, PC, etc.

- DRM system
  - DRM Manager, Trusted Application Agents, Security Agents

- Family Domain
  - Content could be more seamlessly shared amongst all devices owned by a consumer
Thomas S. Messengers et al, “Digital Rights Management in a 3G Mobile Phone and Beyond”, DRM ’03