Digital Rights Management in a 3G Mobile Phone and Beyond

Thomas S. Messerges and Ezzat A. Dabbish
Motorola Lab

2008. 11. 20

2007-30232 이동현

Wireless Networks Lab.
Seoul National University
Contents

• Introduction
• OMA DRM Architecture
• Our DRM System
  – DRM Manager
  – Trusted Application Agents
  – Security Agent
  – DRM Credential
• Security Issues
• Family Domain
• Example Use Case
• Conclusion
Introduction

• How copyright protection of digital items can be securely managed in a 3G mobile phone
• Propose a DRM framework for a 3G mobile phone

• Current mobile phones: 9.6 ~ 19.2 kbps
• 3G mobile phones: 144k ~ 2Mbps
  – Transmission time of a MP3 song: 16 ~ 222 sec.
  – Personal area networking capability (Bluetooth)
    ▪ P2P sharing is possible

• Open Mobile Alliance DRM
  – Problem: consumers wish to use content on any of their devices
OMA DRM Architecture

Cryptographic Chain

Certificate Authority

Right Issuer

Content Issuer

Issue Certificate

Mutual Authentication Using ROAP (RO Acquisition Protocol)

Generate RO (Rights Object)

Generate DCF (DRM Content Format)

Device

Device Cert

RO

DCF

K_{priv}: Private Key
K_{CEK}: Content Encryption Key
K_{REK}: Rights Encryption Key
K_{MAC}: Message Authentication Code Key
OMA DRM Architecture

Protected RO

- **Rights**
  - Content Encryption Key (CEK)
  - Permission
  - Digest of Content
  - Content ID
- **Digital Signature of Rights** (Optional)
- **Rights Encryption Key (REK) and MAC Key**
- **MAC of RO**

**Decryption**
- Encrypted Using REK (Symmetric Key)
- Integrity for DCF
- Authentication, Non-Repudiation, and Integrity for Rights (Domain RO Only)
- Encrypted Using Device’s Public Key
- Authentication, Non-Repudiation, and Integrity for RO (Including REK; Device RO)
Our DRM System

• How to interface the DRM and security S/W with the phone’s OS and applications?
  – To replace I/O elements of the OS that access control mechanisms
  – To use “hyperadvisor” located between OS and hardware
    - invokes the DRM system when trying to access a protected file

• Author’s approach
  – The OS be extended to support DRM functionality
    - Only applications that access DRM-protected content need to be aware of the new DRM extensions
Our DRM System

DRM Manager

- **Authenticate licenses and content**
  - Before using protected digital content
  - Need to verify the integrity and authenticity of the license file
    - Computation of hash in the license file
      - To bind the content to the license
    - Verifying a digital signature of the license

- **Enforce rights**
  - Application can ask the DRM manager
    - play, display, copy, etc.
  - Obtain device’s credentials, check the rights, and approve a particular action

- **Decrypt content**
  - Routes the decrypted content directly to a trusted application agents
    - actually handle the data and are responsible for rendering the content
  - The top-level application will act as the user interface and controller
Our DRM System

Trusted Application Agents

• According to the type of action
  • Rendering agents
    – Provide applications to render the content
    – Provide the low-level drivers that convert the digital data into a format can be consumed by a user
    – Clever API design is needed
  • Transport agents
    – Provide services that move content from one location to another
    – The establishment of a secure authenticated channel with help of security agent
  • Derivative work agents
    – To extract and transform protected content into a different form
    – When duplicating a digital item, installing DRM-protected software
Our DRM System

Security Agents

- Memory and file management
  - Access-controlled file system
    - Store decrypted digital content
    - Store a secure database
    - Store encrypted private keys
  - Memory separation system
    - Guarantee task separation
  - Secure memory system
    - Prevent critical data from leaking out of the system
      - Phone’s private keys, etc.
    - Volatile secure memory is linked to tamper detection circuitry

- Cryptographic operations
  - Protected content: symmetric-key algorithm (AES)
  - Binding between content and licenses: hash algorithm
  - Content key decryption, signature: public-key (RSA or ECC)

- Key management
  - Securely handling a database of the phone’s credentials (keys, certificates, ID)

<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
Our DRM System

DRM Credential

- Serial number
  - Unchangeable number that identifies the phone
- Model number
  - Number that identifies HW and SW version
  - Phone’s capabilities
- Unit private key and Unit certificate
  - used for establishing secure-authenticated channels to a phone
    - KuPri: phone’s unique private key
    - UnitCert: certificate that certifies the corresponding public key (KuPub)
- DRM private key and DRM certificate
  - used exclusively when assigning content to a device
    - KdPri: unique private key
    - DRM Cert: a certificate that certifies the corresponding public key (KdPub)
Security Issues

• License
  – License formats (e.g. XrML, ODRL)
  – Four essential items
    ▪ A value that links the license to the digital item
    ▪ Usage rights
    ▪ A means to decrypt the digital item
    ▪ A signature of the license

• Integrity and authenticity

• Rights enforcement
  – Needs to be able to recognize the version of the license file

• Content protection

• Privacy issues
  – User information must not be disclosed without the explicit consent of the end user
Family Domain

- New concept of content management (proposed)
- Consumers wish to use content on any of their devices
- suitable for devices with limited or no networking capability
  - Device only needs to register with DA once, can be done through a temporary proxy device

```plaintext
Device

Domain Authority (trusted server)

Domain

Device

: KdPri (domain private key)
```
Example Use Case

- Content acquisition

![Diagram showing content acquisition process]

- SAC (Self-Contained Application) exchanges license files with the Content Provider.
- The license file is then used to acquire content for the device.

### Phone Information

- **Phone**
  - Serial Number
  - Model Number
  - Root Key
  - KuPri
  - UnitCert
  - KdPri
  - DRM Cert

- **Identifiers**
  - Permanent
  - Used for authenticating, licenses, servers, etc.
  - Installed by manufacturer

- **3rd-party**
  - Used by others to authenticate the phone
  - Installed by 3rd-party
  - Used to encrypt and decrypt content keys
Conclusion

• Proposed approach offers a good path towards a secure and consumer-friendly DRM system
• Proposed DRM framework is also applicable to other devices
• **Family domain concepts** could be make content be more seamlessly shared