DRM'03

Digital Rights Management in a 3G Mobile Phone and Beyond

Thomas S.Messerges, Ezzat A. Dabbish

Hyojin Yoon
Jaehoon Lee

Contents

- Introduction
- DRM Concepts and strategies
- Our DRM system
  - DRM Manager
  - Trusted Application Agents
  - Security Agent
  - DRM Credential
- Security issues
- Family Domain
- Conclusion

Introduction

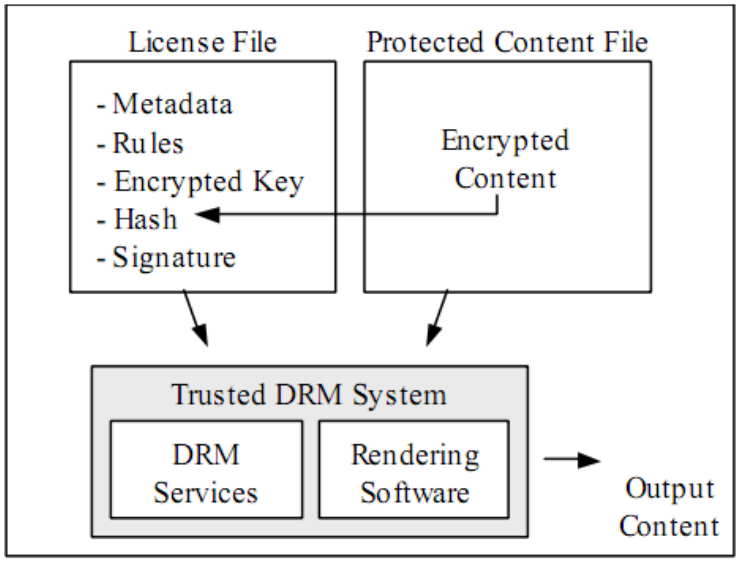
- 3G Mobile Phone
  - High communication rates (144 Kbps ~2 Mbps)
  - Personal Area Networking capability
    - P2P sharing of digital items over short-range networks
  - High Internet Connectivity

- Business opportunities for digital contents are attracting much interest
- Losses from piracy

Digital Rights Management(DRM) will be an essential component for future mobile phones

DRM concepts and strategies - Overview of Trusted DRM System

- License File
  - Metadata
  - Usage Rules
  - Content Encryption Key (CEK)
  - Hash
  - Digital Signature
    - For authenticity and integrity
- Protected Content File (Encrypted)
- DRM System
  - DRM Service
    - Verify the signature & the hash of content
    - Decrypt the content
  - Rendering Software (When content is rendered)



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

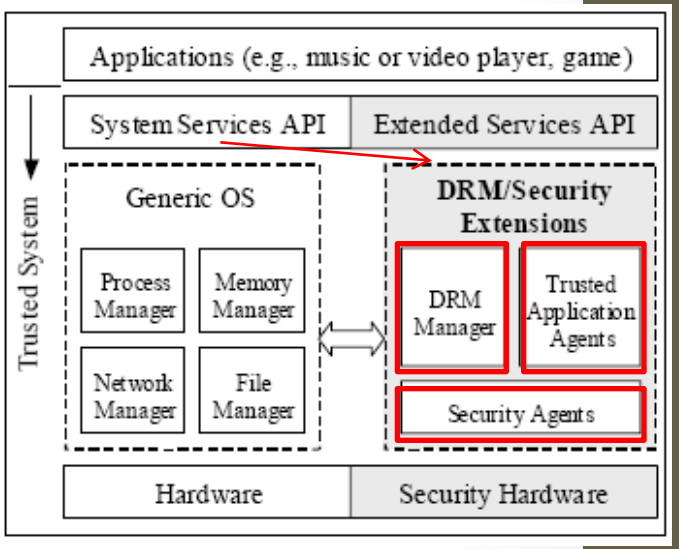
> "Content files **can be distributed** to other devices, but that **licenses** to use this content must be **obtained from a server** called the right issuer"

    - In this paper, **"Family Domain" approach** is proposed
      - 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

- Two approach noted in Schneck's paper
  - Replace the I/O elements of OS with new modules
  - Hyperadvisor

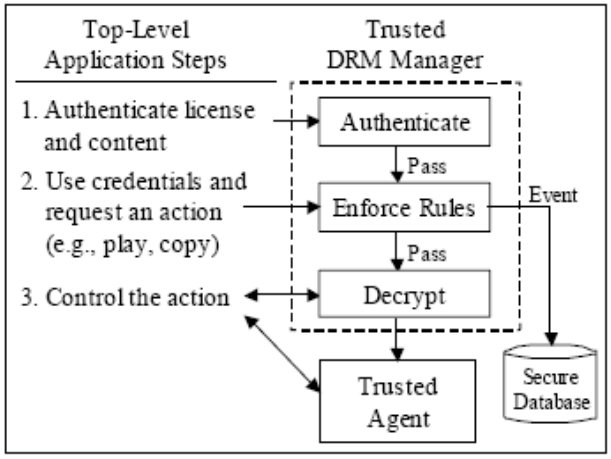
- Our Approach
  - OS is extended to support DRM functionality
  - Access these extended system through API
    - A header indicates if that is protected
    - If file is protected -> call extended API
  - These extensions - "privileged mode"
  - Applications - "user mode"



P.B. Schneck, "Persistent Access Control to Prevent Piracy of Digital Information", Proceedings of the IEEE'99

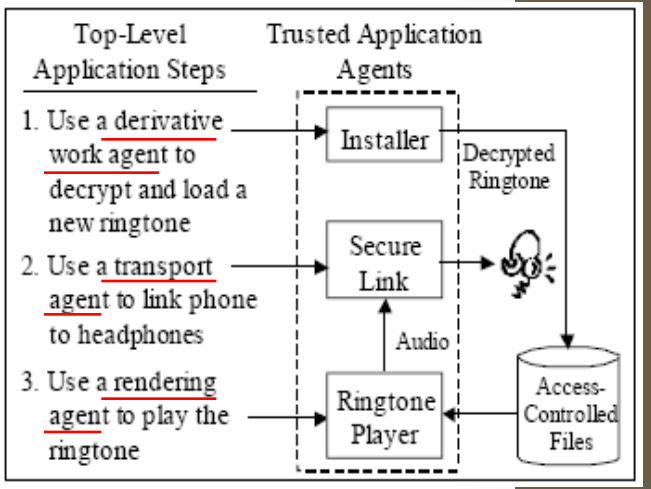
OUR DRM SYSTEM - DRM manager

- Authenticate Licenses and Content
  - Verify Cryptographic hash of the license file
  - Digital signature
    - With the help of Security Agents
- Enforce Rights
  - **Action**s 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
      (e.g., keys, certificates, IDs)
  - Perform additional event for an action
- Decrypt Content
  - **Decrypt** the content using key
  - Route it to a trusted application agent



OUR DRM SYSTEM - Trusted Application Agents

- **Actually** Access and manipulate decrypted content



- Rendering Agents
  - **Render** DRM-protected content
    - e.g., a music player, a picture viewer, an application loader
- Transport Agents
  - **move** content from one location to another
    - e.g., email attachments, messaging services, streaming
  - Establish a Secure Authenticate Channel(SAC)
    - e.g., secure Bluetooth link b/w the phone and the headphones
- Derivative Work Agents
  - **Extract and transform** protected content or license into a different form
    - e.g., digital item duplication
  - **Installation** of DRM-protected software or data
    - For fast execution, installed software and data is decrypted and this makes it vulnerable to copying
    - Place the decrypted data into **an access-controlled file system** maintained by security agents

DRM System – Security Agents[1/2]

- Handle the security-related functions
  - Memory and File management
  - Cryptographic operations
  - Key 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**

DRM System – Security Agents[2/2]

- 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)

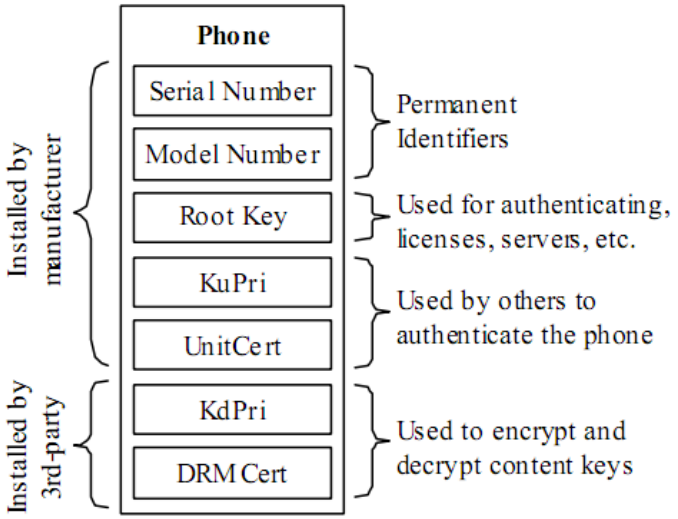
Operation	Time
Hash of a license (5KByte)	SHA1: 3 ms
Verify license signature	RSA(1): 100 ms ECC(2): 150 ms
Decrypt content key	RSA(1): 1,800 ms ECC(2): 90 ms
Decrypt content (2 Kbyte)	AES(3): 1.6 ms

(1) 1024-bit RSA with CRT (2) WTLS Curve 3 (3) 128-bit key

- Key/certificate Manager
  - Securely handle a database of the phone's credentials
    - Keys, Certificates, IDs
  - Parsing and verifying the appropriate certificates

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 Authenticate Channel(SAC) to a phone
  - KdPri and DRMCert
    - Used for assigning content to a device

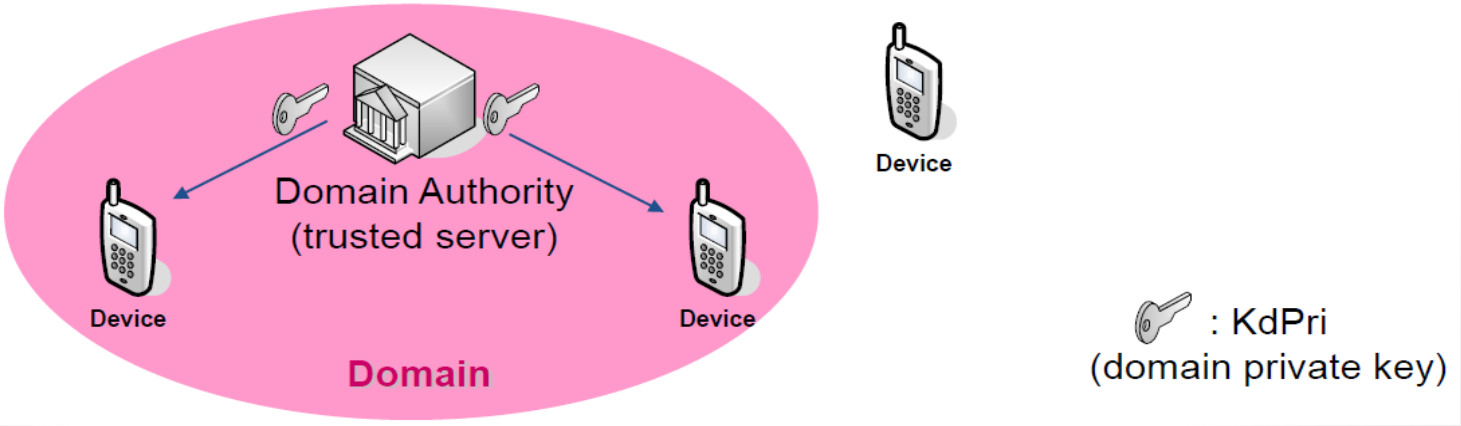


Security Issues

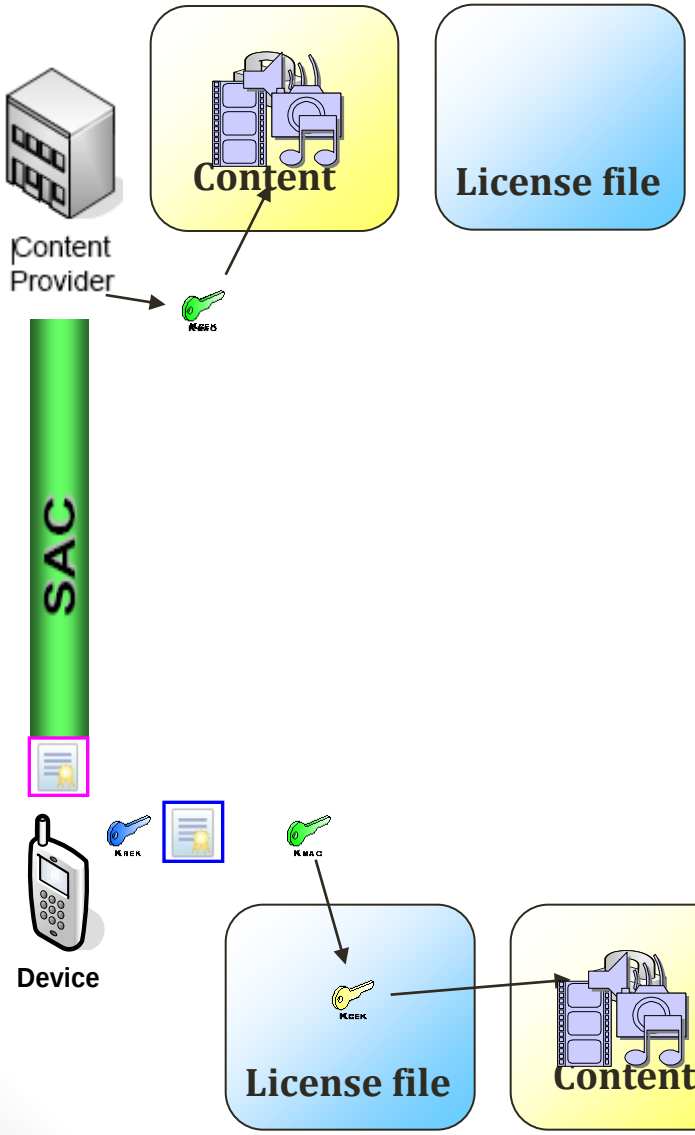
- Licenses
  - Need to verify integrity and authenticity of licenses
- Integrity and Authenticity
  - Content providers need to trust that the DRM system will keep keys secret
- Rights Enforcement
  - DRM manager should enforce rights responsibly and fail in a safe manner if there are conflicting constraints
- Content Protection
  - Rendering software should be trusted to not leak of copy the decrypted content
- Privacy Issues
  - User information and identity must not be disclosed

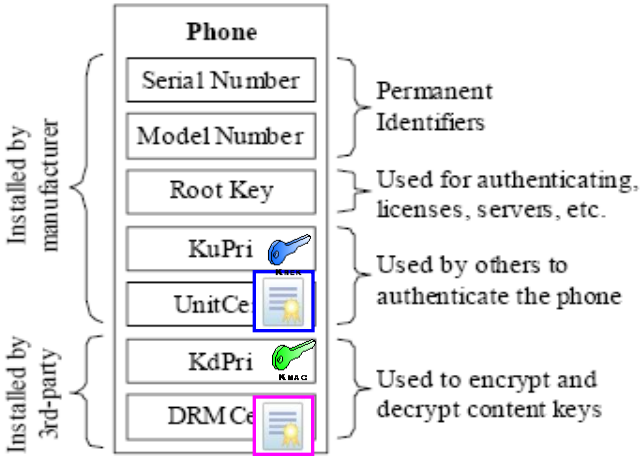
Family Domain

- 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



Example Use Case





K_{PRIV}: Private Key

K_{CEK}: Content Encryption Key

K_{REK}: Rights Encryption Key

K_{MAC}: Message Authentication Code Key

Conclusion

- DRM framework is proposed for a mobile phone environment
  - Also applicable to other devices
    - PDA, tablet pc, automobile 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

Reference

- Thomas S. Messergers et al, “**Digital Rights Management in a 3G Mobile Phone and Beyond**”, DRM ‘03