모바일 환경에서 효율적 디지털 콘텐츠 유통을 위한 서비스 방법

(A service scheme for the efficient digital contents distribution in mobile environments)

김 영 희*, 이 창 열**
(Young-Hee Kim, Chang-Yeol Lee)

요 약 모바일 기기 사용 환경에서 디지털 콘텐츠에 대한 권리를 보호하고 안전하게 사용하기 위한 방법으로 PKI 기술을 이용하였다. 암호화는 TripleDES를, 전자서명은 RSA를 사용하였으며, 효과적 관리를 위한 구조로 암호화된 콘텐츠와 서비스를 위한 정보를 연계하는 메카니즘을 제시하였으며, 이를 바탕으로 콘텐츠를 안전하게 유통하는 모바일 환경을 제시하였다. 본 연구를 통하여 콘텐츠에 대한 권리를 효과적으로 보호할 수 있으며, 안전한 모바일 콘텐츠 유통 환경을 제시하였다.

핵심주제어 : 디지털 콘텐츠, DRM, 암호화, 전자서명, 권리 관리

Abstract We use PKI technology for the digital content distribution in mobile environment. Encoding method is used TripleDES and digital signature is used RSA. For the efficient methods and processes to the digital content distribution, we proposed the mechanism which consists of the sequential steps including the digital contents encoding step, rights management information signature step, and interconnection steps. As a result of this study, we propose the efficient and safe processes for the mobile content distribution environment.

Key Words : Digital Content, DRM, encoding, Digital Signature, Rights Management

1. 서 론

최근 무선 이동통신의 급속한 발달로 인해 다양한 기능을 제공하는 모바일 기기를 이용하여 디지털 콘텐츠의 이용 및 유통이 증가하고 있다. 또한, 디지털 콘텐츠를 위한 유무선 전송환경이 발전됨에 따라 기존 오프라인에서 서비스 되던 음반, 영화, 책, 방송 등이 제약된 시간과 장소를 초월하여 자신이 원하는 시간과 장소에서 자유롭게 사용 가능하게 되었고, 외장형 메모리 사용량 의 증가와 메모리 가격 하락으로 인해 모바일 서비스 이용의 다변화를 가져왔다. 반면, 모바일 콘텐츠의 사용을 위해 무선 인터넷 이용료 및 콘텐츠 구입의 비용은 모바일 인터넷 사용자의 부담을 가중 시키고 있기 때문에 이용에 대한 많은 제약을 가져오고 있다. 이러한 비용의 최소화를 위해 PC통신을 이용하여 콘텐츠를 모바일 기기로 제공하는 방법과 이를 제공하기 위해 서로 다른 디바이스 간의 콘텐츠 이용의 편리성이 대두되고 있다. 이러한 방법은 콘텐츠 이용에 드는 통신의 비용을 최소화하고

* 성균관대학교 컴퓨터공학과 박사
** 동의대학교 컴퓨터공학과 교수

콘텐츠 이용의 확산을 가져오는데 유용하지만, 콘텐츠 저작자의 지적 재산권 보호 및 유료 콘텐츠의 안전한 배포 등의 불법적인 유포를 방지하기 위한 새로운 유형의 콘텐츠 보안 기술이 요구되어진다. 디지털 콘텐츠 보호 기술은 저작권 보호를 위한 기술[1][2]과 복사 방지를 위한 암호화/복호화, 인증기술을 필요로 한다. 이를 위해 본 논문에서는 콘텐츠 공급자로부터 제공되는 디지털 콘텐츠에 지불비용(Payload), 사용기간, 사용횟수 등의 불법복제에 대해 사용자 제한을 적용하여 사용자 PC 또는 모바일 외장 메모리로 다운로드 후 발생되는 제3자로의 불법복제 방지를 가능하도록 하는 모바일 콘텐츠 보안 기법을 제시하고자 한다. 따라서 콘텐츠 공급자는 제공되는 콘텐츠에 복사 방지를 위한 암호 기술과 사용제한을 위한 인증 기술을 적용한다. 그리고 웹 서비스에 의해 사용자에게 제공 후, 콘텐츠 사용자는 서비스 이용이 저렴하고 콘텐츠의 이동이 자유로운 PC 및 외장형 메모리로부터 모바일 기기에 맞는 파일 변환 후, 저비용의 다양한 서비스를 제공받는다. 그 결과 콘텐츠 공급자는 모바일 기기 환경의 무선 데이터 송수신을 위한 다양한 콘텐츠 확보 및 제공을 통해 활발한 저작 활동을 할 수 있고, 콘텐츠 사용자는 모바일 콘텐츠 구입에 드는 비용을 최소화하여 콘텐츠 사용료에 부담을 해결하므로 안전하게 콘텐츠를 사용 가능하도록 할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 디지털 콘텐츠 보안 기법에 대한 연구를 살펴보고, 3장에서는 본 논문에서 제안하는 디지털 콘텐츠 보안 기법을 이용한 보안 프로그램 매커니즘 및 세부 프로토콜을 설명하고, 4장에서는 구현을 통해 디지털 콘텐츠의 암호화된 패키징 결과를 보인다. 5장에서는 결론 및 향후 과제에 대해 기술한다.

2. 관련 연구

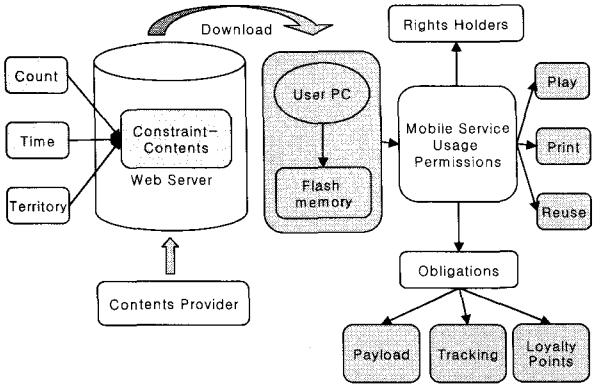
모바일 기기를 이용하여 제공되고 있는 디지털 콘텐츠는 그림 1과 같이 콘텐츠 공급자(CP)로부터 제공되는 콘텐츠에 사용기간, 사용 횟수 등의 불법복제에 대해 사용자 제한을 적용하여 사용자 PC 또는 모바일 외장 메모리로 다운로드 후 발생되는 불법복제 방지를 위해 저작권 보호를 가능하게 하고자 한다. 이를 위해 모바일 기기 상에서 운용되는 동영상 콘텐츠 3GP, MP4 등에 저작권 및 불법 유통을 방제하기 위해서 DRM(Digital Rights Management)[3][4]의 핵심 기술중 암호화 / 복호화(encryption/decryption) 기법 및 인증(authentication)기법을 적용하여 콘텐츠 보안 프로그램들이 개발되고 있다. 콘텐츠 보안은 네트워크상에서 다양한 콘텐츠 제공자로부터 고객으로 안전하게 전달하고 고객이 불법적으로 사용하지 못하도록 하는 시스템 기술이다. 가장 중요한 기술은 암호화 기술 즉, 고객 컴퓨터 고유번호를 암호키로 사용하여 콘텐츠를 암호화하여 전달하고 이를 제3자에게 전달하여도 쉽게 노출되지 않도록 하는 것이 가장 중요하다. 기존의 콘텐츠 전달 시스템은 사용자 ID와 비밀번호를 사용하는데 이러한 경우 ID와 비밀번호를 공유하므로써 손쉽게 콘텐츠를 불법으로 사용가능하므로 이러한 문제점을 해결하기 위해 PKI나 DSA등의 다양한 보안 기법을 적용한다. 따라서, 여러 가지 핵심 기술 중에서 본 연구를 위해 디지털 서명(Digital Signature) 기법과 콘텐츠 보호[5]를 위한 암·복호 기법[6][7][8][9]에 대해 살펴 보고자 한다.

2.1 Digital Signatures

본 연구를 위한 보안 기법을 살펴보면 다음과 같다.

2.1.1 전자 서명의 특징

메시지 인증(message authentication)은 메시지를 교환하는 두 주체를 제삼자로부터 보호하지만, 메시지 송신자와 수신자 사이의 완전한 신뢰를 위해 디지털 서명(Digital Signature)을 사용한다. 디지털 서명은 시간, 날짜, 작성자, 시간에 대한 Content에 대하여 인증하며 분쟁을 해결하기 위해 제3의 기관에 의한 증명이 가능해야 한다. 전자 서명의 접근 방식은 direct Digital Signature 방식과 arbitrated Digital Signature의 두 범주로 나뉜다. direct Digital Signature는 송신자의 개인키로 전체 메시지를 암호화하거나, 송신자의 개인키로 메시지의 해시코드를 암호화하여 생성한다. 기밀성은



<그림 1> Mobile Contents Usage Model

대칭키 암호화 방식의 공유된 개인키나 공개키 암호화 방식의 수신자의 공개키를 이용하여 암호화된 전체 메시지에 서명을 추가하므로 제공된다. 이 구조의 유효성은 개인키의 security에 의존적이므로 취약한 문제가 제기된다. 반면 Arbitrated Digital Signature는 중재자를 사용하는 방법으로 모든 통신주체들은 arbitration mechanism이 적절하게 동작함에 따라 신뢰의 정도를 높일 수 있다.

2.1.2 Arbitrated Digital Signature

Arbitrated Digital Signature의 종류는 그림 2와 같이 나타낼 수 있다. 그림 2의 (a)는 symmetric encryption이 사용된다. 송신자를 X, 중재자를 A라 가정하면 송신자와 중재자 사이의 비밀키는 Kx_a로 나타내며, X는 메시지 M을 구성하고, 이에 대한 해시값 H(M)을 계산한다. 그리고 X는 A에게 서명이 첨가된 메시지를 보낸다. 서명은 Kx_a를 사용하여 암호화된 해시값을 더한 X의 식별자 IDx로 구성된다. A는 서명을 복호화하고, 메시지의 유효성을 검증하기 위해 해시값을 검사한다. 그런 다음 A는 K_{ay}를 사용하여 암호화된 메시지를 Y에게 전송한다. Y에게 전송된 메시지에는 ID_x, X로부터 온 원본 메시지, timestamp가 포함되어 있다. Y는 전송받은 메시지와 서명을 복구하기 위하여 복호화를 수행한다. timestamp는 메시지가 시간적으로 올바르게 존재하도록 하며, replay시도를 막는다. Y는 M과 signature를 저장하고, 분쟁 시에 Y는 자신이 받은 M에 대한 권리를 주장할 수 있다. (b)는 중재를 제공할 뿐만 아니라 기밀성을 보장해 준다. X와 Y가 공유하는 비밀키를 K_{xy}라고 가정한다. 그렇다면, X는 K_{xy}로 암호화된 메시지의 복사본, 식별자, 서명을 A에게 전송한다. 서명은 K_{xa}로 암호화된 메시지의 해시값에 식별자를 더하여 구성된다. A는 서명을 복호화하고, 메시지가 유효한 지를 검증하기 위하여 해시값을 검사한다. A는 메시지의 암호화된 버전을 가지고만 작업을 하고, 따라서 메시지를 읽는 것을 막을 수 있다. 이후에 A는 X로 받은 모든 것에 K_{ay}로 암호화된 timestamp를 더하여 Y에게 전송한다. 그림 2의 (c)는 연산 과정 및 요구사항은 메시지를 읽을 수 없음에도 불구하고, 중재자는 X나 Y 중 하나의 불법행위를 막을 수 있다. 시나리오를 공유하는 경우에 생길 수 있는 문제로 중재자가 메시지에 대한 서명을 거부하는 송신자와 협력하거나 송신자의 서명을 위조하려는 수신자와 협력하려는 것이다. 이런 문제를 공개키 과정으로 해결한다.

(1) $X \rightarrow A : M \| E_{Kxa}[IDx \| H(M)]$
(2) $A \rightarrow Y : E_{Kay}[IDx \| M \| E_{Kxa}[IDx \| H(M) \| T]$

(a) Conventional Encryption, Arbiter Sees Message

(1) $X \rightarrow A : ID_x \| E_{Kxy}[M] \| E_{Kxa}[IDx \| H(E_{Kxy}[M])]$
(2) $A \rightarrow Y : E_{Kay}[IDx \| E_{Kxy}[M] \| E_{Kxa}[IDx \| H(E_{Kxy}[M])] \| T]$

(b) Conventional Encryption, Arbiter Does not See Message

(1) $X \rightarrow A : IDx \| E_{KRx}[IDx \| E_{KUy}(E_{KRx}[M])]$
(2) $A \rightarrow Y : E_{KRa}[IDx \| E_{KUy}[E_{KRx}[M]] \| T]$

(c) Public-Key Encryption, Arbiter Does Not See Message

<그림 2> Arbitrated Digital Signature Techniques

2.2 Authentication Protocols

2.2.1 Symmetric Encryption Approach

대칭형 암호의 키에 대한 두 단계의 계층 구조는 분산 환경에서 기밀성을 제공한다. 이들 전략은 KDC에 의한 Trust Key를 사용하는 것이다. 즉 각 통신개체는 KDC에 의해 master key라고 알려진, 비밀키를 공유하고, KDC는 세션키로 알려진 두 접속 개체사이의 Short time에 키 생성에 대해

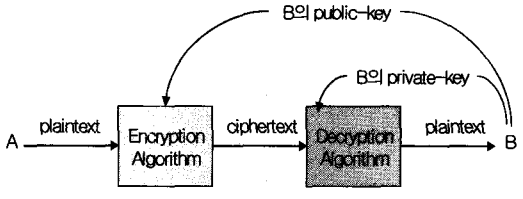
책임을 지고 키 배포를 보호하기 위해 master키를 사용해 이들 키를 배포한다. 그림 3은 KDC를 사용해 비밀키를 배포하는 Needham과 Sohroeder의 초기에 제안한 프로토콜을 나타 낸다.

$A \rightarrow KDC : ID_A \parallel ID_B \parallel N_1$
$KDC \rightarrow A : E_{Ka}[K_s \parallel ID_B \parallel N_1 \parallel E_{Kb}[K_s \parallel ID_A]]$
$A \rightarrow B : E_{Kb}[K_s \parallel ID_A]$
$B \rightarrow A : E_{Ks}[N_2]$
$A \rightarrow B : E_{Ks}[f(N_2)]$

<그림3> Symmetric Encryption Protocol

2.2.2 Public-Key Encryption Approach

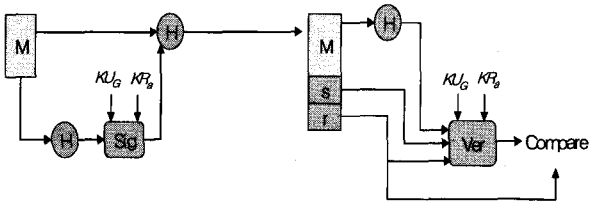
공개키 암호화 기법은 그림 4와 같이 메시지를 암호화할 때 사용하는 암호화 키와 그 암호문을 해독할 때 사용하는 해독 키가 서로 다른 암호화 시스템을 말한다. 송신자 A가 수신자 B에게 암호문을 전송하려 할 경우, 수신자 B의 암호화 키는 공개하며 B의 해독 키는 B만이 비밀로 유지한다. 암호화 키가 공개되어 있으므로 누구나 메시지를 암호화하여 B에게 전송할 수 있지만, 그 암호문의 해독은 B만이 할 수 있다. 이 기법의 대표적인 것으로는 RSA 방식이 있다. 이 기법은 관용 암호화 기법과 비교하여 암호화 및 해독 속도는 상대적으로 느린 반면에 암호화 키를 공개함으로써 키의 생성 및 분배가 용이하다. 실제로는 공개키 암호화 기법과 관용 암호화 기법이 보통 함께 결합되어 사용되며 공개키 기법을 이용하여 임시적으로 사용될 비밀 세션 키를 전달한 후에 이 세션 키를 이용하여 관용 암호화 방식으로 메시지를 암호화하여 전송하는 방식을 들 수 있다.



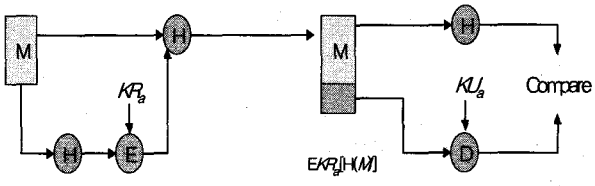
<그림 4> Public-Key Encryption Technique

2.2.3 Digital Signature 접근 방식

전자 서명을 위한 접근 방식은 DSS 접근 방식과 RSA 접근 방식을 사용한다. DSS는 그림 5에 (a)에서 보는 바와 같이 digital Signature 함수를 제공하기 위해 설계된 알고리즘으로 RSA와 다르게 암호화나 Key 교환을 사용할 수 없지만, 공개키 기술을 사용한다. DSS 접근 방식은 해시 함수를 사용하며 해시코드의 생성을 위해 특정한 서명으로 생성된 임의 값 K가 서명함수의 입력이 된다. 서명 함수는 송신자의 개인키와 통신 주체들의 그룹에 알려진 매개변수 집합에 의존적이다. 여기서 이들 집합을 구성하는 global public key(KU_G)를 고려할 수 있고, 2개의 컴포넌트로 구성된 s 와 r을 덧붙인다. 수신 측에서는 입력 메시지의 해시코드를 생성한다. 여기에 서명을 더하면 검증함수의 입력이 되고 검증함수는 global public key 뿐만 아니라 송신자의 공개키(KU_a)에도 의존적이다. 검증 함수의 출력은 서명이 유효하다면 컴포넌트 r의 서명과 동일한 값이다. 서명 함수는 개인키를 알고 있는 송신자만이 유효한 서명을 생성 할 수 있다. 반면, RSA 접근 방식은 그림 5에 (b)와 같이 서명된 메시지가 해시함수의 입력이 되고 해시함수는 고정된 길이의 해시코드를 생성한다.



(a) DSS Approach



(b) RSA Approach

<그림 5> Digital Signature의 두가지 접근

이들 해시코드는 송신자의 개인키를 사용해 암호화된 서명 형태이다. 메시지와 서명이 모두 전송되고, 수신자는 메시지를 받아서 해시코드를 생성한다. 수신자는 송신자의 공개키를 사용하여 서명

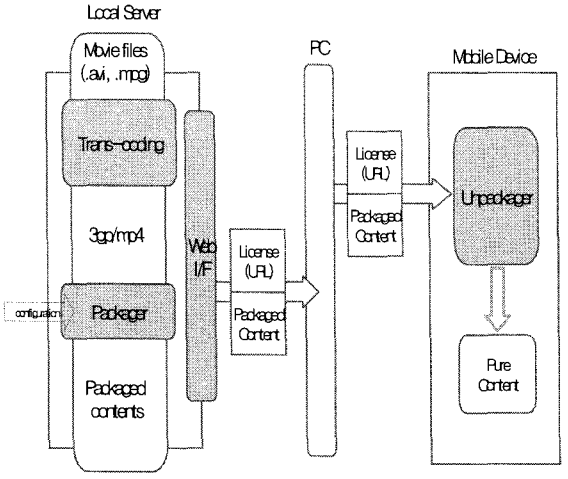
을 복호화 한다. 만일 계산된 해시코드와 복호화된 서명이 일치한다면 서명은 유효하다고 인정하는 방식이다.

3. 디지털 콘텐츠 서비스 보안 기법

최근 모바일 서비스를 이용하는 단말기의 대부분이 데스크 탑 PC에서 무선 단말기인 PDA 및 모바일 폰 등으로 변화해 가며 기존 DRM을 무선 단말기 등에 적용하고자 하는 요구가 늘어나고 있다. 본 논문에서 제안하는 모바일 환경에서 무선 콘텐츠를 제공 받기 위한 서비스 보안 기법은 다음과 같다.

3.1 시스템 구성도

디지털 콘텐츠 보안 서비스를 위한 전체 시스템 구성도는 그림 6과 같다.



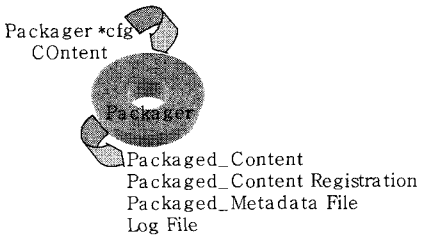
<그림 6> 모바일 서비스 보안 프로그램 전체 구성도

(1) Trans-Coding

데스크 탑 PC에서 사용되는 콘텐츠에 대하여 디지털 콘텐츠 서비스로의 콘텐츠 변환을 위해 X4live Converter, Xvideo Converter, Stoikvideo Converter10 등과 같은 동영상 파일 변환 프로그램을 적용한다.

(2) Packager

패키저는 콘텐츠를 허가된 사용자만이 이용할 수 있도록 암호화하는 과정을 수행한다. 패키징된 결과로 그림 7과 같이 Packaged_Content, Packaged_Content Registration, Log 파일 Packaged_Metadata File을 생성한다.



<그림 7> 패키저

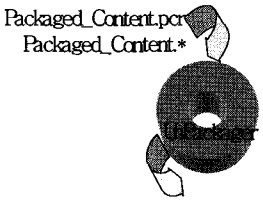
Packager.cfg는 환경 정보가 저장된 파일로서, 표1과 같은 정보가 저장되어 있다.

<표 1> 패키저 환경 파일 정보

File 정보
· Content : Pure Content · Packaged_Content :DRM Content · Packaged_Content Registration : 패키징 결과에 따라 발생되는 파일로 클리어링하우스에 등록할 내용 · Packaged Metadata File : Local Server에 제공되는 파일 · Log File : Packager.cfg로부터 얻은 정보

(3) Unpackager

언패키저는 패키징을 풀기 위한 과정을 수행한다. 패키지을 풀기 위해 Packaged_Content.Pcr을 필요로 하며 .pcr 파일로부터 Key를 생성하여 패키징된 콘텐츠를 푼다. 언패키징의 결과로 그림 8과 같이 Pure Content와 Header 파일을 생성한다. 생성된 각각의 파일 정보는 표 2와 같다.



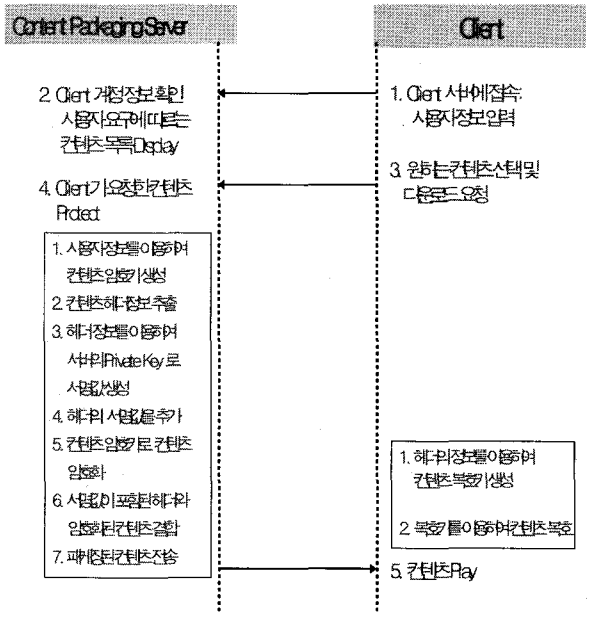
<그림 8> 언패키저

<표 2> 언패키저 생성 파일 정보

File 정보
· Packaged_Content :DRM Content · Packaged_Content Registration : 패키징 결과에 따라 발생되는 파일 · Pure Content : 원시 Content · Header File : Header File 정보

3.2 콘텐츠 서비스 보안 메커니즘

콘텐츠 서비스 보안 매커니즘은 서버와 클라이언트로 나누어 구성된다. 서버의 운영체제로서 리눅스 또는 윈도우즈 NT 모두 포팅이 가능하며 클라이언트는 윈도우즈 계열로 전제한다. 그림 9는 콘텐츠 보안 서비스 구성도이다.



<그림 9> 콘텐츠 보안 서비스 메커니즘

서비스는 사전 단계와 서비스 5단계로 나누어지며, 기본 단계에서는 콘텐츠 보안 사전 협의와 서버의 개인키, 공개키쌍 생성 및 공개키 공개 단계이며, 서비스 5단계에서는 실제적인 콘텐츠 보호 서비스를 실행한다.

(1) 콘텐츠 보안 사전 협의

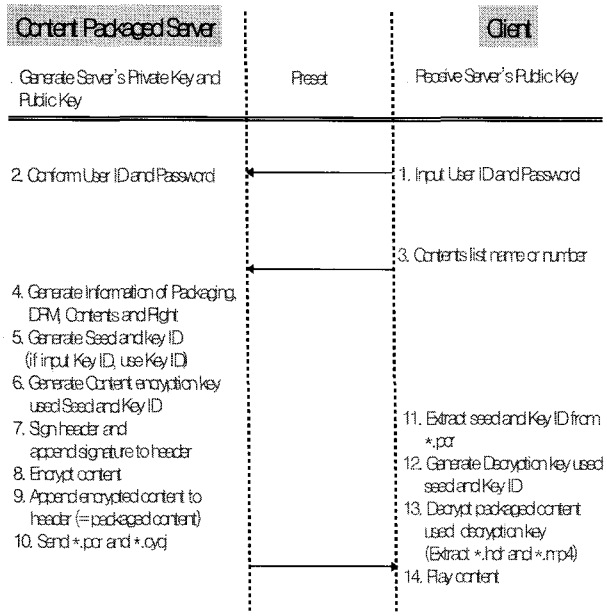
① 서버는 자신이 사용할 콘텐츠 서명용 개인키와 공개용 공개키 쌍을 생성하여, 개인키는 서버의 고유 영역에 저장하고, 공개키는 공개한다.
② 서비스 이용자는 서비스 제공자에게 자신의 실명확인과 함께 자신의 정보로 사용자 등록을 한다. (ID와 패스워드를 부여 받음)
③ 자신의 컴퓨터 및 모바일 기기에서 패키징 콘텐츠의 언패키징 시 필요한 암/복호화 알고리즘과 서명, 검증 알고리즘을 지정한다.

(2) 콘텐츠 보호 서비스

① 사용자는 서버에 접속하여 자신의 ID와 패스워드를 이용하여 사용자 인증을 받는다.
② 서버는 사용자가 정식 사용자임을 확인 후, 서버가 보유하고 있는 콘텐츠의 목록을 사용자에게 전송한다.
③ 사용자는 콘텐츠 목록에서 자신이 다운로드 할 콘텐츠를 선택하여 서버로 전송한다.
④ 서버는 사용자로부터 수신된 콘텐츠 목록을 탐색하여, 각각 또는 전체를 패키징 한다. 그리고 클라이언트에게 패키징한 콘텐츠를 전송한다.
⑤ 클라이언트는 수신된 패키징 콘텐츠를 언패키징하여 콘텐츠를 실행한다.

3.3 세부 프로토콜

본 절에서는 프로토콜별 세부 내용을 설명한다. 서비스는 사전 3단계와 서비스 14단계로 나눈다. 그림 10은 서비스 단계에 따른 데이터의 흐름을 나타낸다.



<그림 10> 서비스 단계에 따른 데이터의 흐름

(1) 사전 단계

① 서버는 서비스 시작 전에, 서버의 개인키와 공개키 쌍을 생성하여 개인키는 서버의 고유한 장소에 보관하고, 공개키는 공개한다. 이때, 개인키는 콘텐츠 패키징 단계에서 콘텐츠 헤더를 서명하는 사용되고, 공개키는 클라이언트에서 서명값을 검증하는데 사용한다. 공개키는 공개키 서버를 이용하는 방식 또는 클라이언트로 패키징을 통해 전송하는 직접 전송방식을 이용한다.

② 사용자는 서버에게 자신의 고유 정보를 입력하고 사용자 등록을 한다. 이때, 서버와 클라이언트가 사용할 콘텐츠 암/복호 알고리즘과 서명, 검증용 알고리즘을 협상한다. 본 논문에서는 암/복호 알고리즘으로 TripleDES와 서명 알고리즘으로 RSA를 이용한다.

③ 서버는 사용자에게 ID와 패스워드를 설정하여 주고, 이를 근거로 사용자를 관리한다.

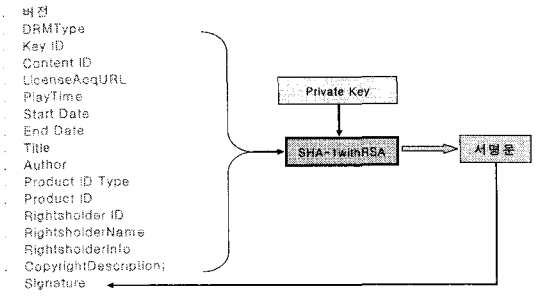
(2) 서비스 단계

① 클라이언트는 서버에 접속하여, 자신의 ID와 패스워드를 전송한다.

② 서버는 자신이 보유한 클라이언트 DB에서 서버에 접속한 사용자가 정식 사용자 인지 확인한다. 정식 사용자임이 확인되면, 보유한 콘텐츠 목록을 클라이언트에게 전송한다.

③ 클라이언트는 콘텐츠 목록 중에서 원하는 콘텐츠를 선택한 후, 그 목록을 서버로 전송한다.

④ 서버는 사용자가 요구한 콘텐츠 목록을 확인하고, 콘텐츠별 정보를 각각 추출한다. 추출한 정보를 이용하여 콘텐츠의 헤더를 생성하고, 헤더의 마지막 필드에 콘텐츠 헤더 정보를 서버가 서명한 서명값을 덧붙인다. 콘텐츠 헤더에는 패키징, DRM 그리고 저작권 정보가 포함되어 있고, 헤더 정보 서명에는 서버의 개인키를 이용한 SHA-1 with RSA 알고리즘이 사용된다. 그림 11은 콘텐츠 패키징의 헤더부를 나타낸다.



<그림 11> 콘텐츠의 헤더에 포함된 정보

⑤ 서버는 콘텐츠 암/복호에 사용할 비밀키를 생성하기 위해, KeyID와 SEED 값을 생성한다. KeyID와 SEED는 관리자가 직접 입력한 값을 이용하거나 자동생성 방법을 이용한다.

⑥ KeyID와 SEED 값을 입력으로 Key Generator를 통해 키를 생성한다. 콘텐츠 암/복호용 키는 콘텐츠 패키징 후 자동 삭제된다.

⑦ ④단계에서 생성한 서명용 개인키를 이용하여, 콘텐츠의 헤더정보를 서명한다.

⑧ ⑥단계에서 생성한 콘텐츠 암/복호용 비밀키와 콘텐츠를 입력으로 TripleDES를 통해 콘텐츠를 암호화 한다. 그림 12는 서버에서 클라이언트로 전송될 콘텐츠 패키징의 암호화 과정을 나타낸 것이다.

⑨ ⑦과 ⑧단계에서 생성한 헤더와 암호화된 콘

텐츠를 덧붙인다. (콘텐츠 패키징)

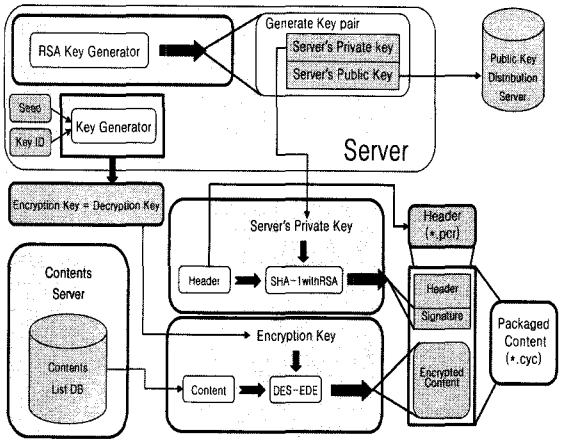
⑩ 패키징된 콘텐츠를 클라이언트에게 전송한다. 패키징된 콘텐츠의 내부 구조는 그림 13과 같다.

⑪ 수신된 패키징을 서버의 공개키를 이용하여 헤더의 무결성을 검증한 후, 이상이 없으면 패키징의 헤더부에서 KeyID와 SEED를 추출한다.

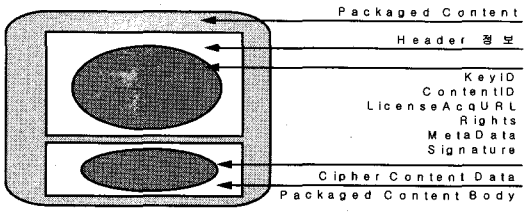
⑫ 추출한 KeyID와 SEED를 이용하여 패키징 복호키를 생성한다.

⑬ 콘텐츠복호키를 이용하여 콘텐츠를 복호한다. 그림 14는 클라이언트가 수신한 패키징된 콘텐츠를 언패키징하는 과정을 나타낸다.

⑭ 복호된 콘텐츠를 실행한다.



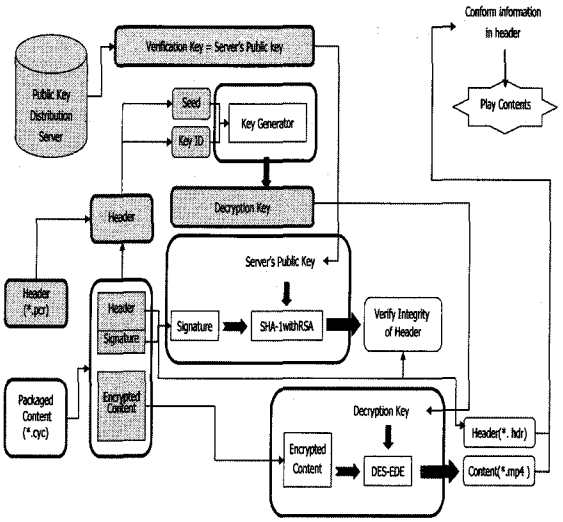
<그림 12> 콘텐츠 암호화 프로세싱



<그림 13> 패키징된 콘텐츠 내부 구조

4. 구현 결과

본 장에서는 앞에서 제안한 콘텐츠 서비스 보안 기법을 적용하여 원형의 콘텐츠 정보가 암호화된 패키징 결과와 패키징된 결과를 언패키징 하는 결과를 보였다.



<그림 14> 콘텐츠 복호화 프로세싱

4.1 개발 환경

본 연구의 수행을 위한 개발 환경은 Linux Fedora 4 운영체제 환경에서 Java SDK1.4.2와 JCE1.2.2(Java Cryptography Extension)을 이용하여 구현하였다. 제안하는 보안 서비스 프로그램의 요구사항은 다음과 같다.

- 일반화 : 패키저의 확장성
- 사용의 편리성
- XML 기반의 결과물 제공
- Linux 플랫폼에서 동작
- 로그 정보 제공
- 라이센스 정보 전자 서명

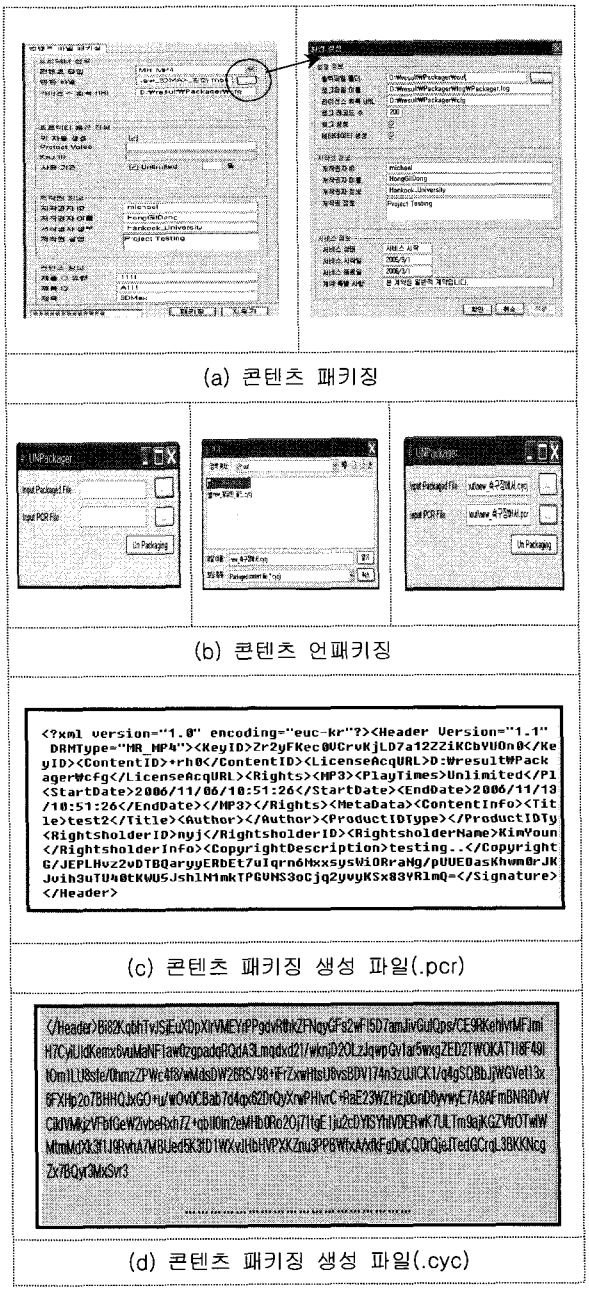
4.2 결과

그림 15 (a)는 구현된 패키징 프로그램의 실행 초기 화면, 환경 정보 설정, 패키징된 결과 및 로그 파일 등이 생성될 경로, 키 생성 서버의 URL 설정, 기타 저작권 정보, 서비스 정보 설정을 나타내고, 그림 15 (b)는 암호화된 콘텐츠에 대하여 인증과정을 거쳐 복호화 하는 프로그램을 실행한 결과로 패키징 결과 생성 후 암호화된 콘텐츠 파일, PCR 파일을 로딩 후 언패키징을 수행하는 과정을 나타낸다. 그 결과 그림 15 (c), (d)와 같이 .pcr 파

일, 암호화된 콘텐츠 파일 정보인 .cyc 파일 결과를 생성 한다. 생성된 .pcr과 .cyc정보는 다음과 같다. <DrmValue_S Naming="Seed">는 복호키 생성에 사용되는 seed로 서버에서 랜덤하게 생성되고, <DrmValue_C Naming="KeyID">는 복호키 생성에 사용되는 KeyID이다. <VerificationKey Encoding="Base64">는 서명된 내용을 검증하기 위해 사용되는 공개된 Public Key, <TimeStamp>는 콘텐츠가 Protected된 시간 정보, 콘텐츠 암호화를 위해 입력된 사용자 정보와 DRM 정보 + 서명값을 갖는 헤더 정보, 암호화 알고리즘에 의해 콘텐츠의 원형이 암호화된 내용의 콘텐츠이다. 사용자에게 전송되는 패키징화된 콘텐츠의 정보를 담고 있는 서명이 추가된 헤더와 암호화된 콘텐츠를 연결하여(concatenate)하여 전송하게 되고, 이러한 콘텐츠는 사용자 측면에서 사용전에 인증 과정을 거쳐 복호키로 콘텐츠를 복호하여 사용하게 된다.

5. 결론 및 향후 과제

본 논문은 모바일 기기에서 디지털 콘텐츠를 안전하게 제공할 수 있는 디지털 저작권 보호 및 불법 복제 방지를 위한 보안 서비스 기법에 대하여 제안하였다. 이를 위하여 콘텐츠에 복사 방지를 위한 암호 기술과 사용제한을 위한 인증 기술을 적용하였다. 디지털 콘텐츠 서비스 보안 기법은 콘텐츠 공급자에 의해 제공되는 대상 콘텐츠를 암호화하고 사용자가 요청하는 DRM 정보 등을 암호화된 콘텐츠와 함께 패키징하여 전송한다. 패키징된 콘텐츠는 사용시에 정보의 위조를 확인하기 위해 인증 과정을 거쳐 무결성을 검사하고, 신뢰성이 확보되면 복호화 과정을 통해 사용자 측에서 요구한 기간이나 횟수에 대하여 사용에 대한 권한을 부여한다. 따라서 PKI 기반의 안전한 패키징을 통해 모바일 환경에서 제공되는 디지털 콘텐츠에 대한 이용 권한 통제 및 콘텐츠 보호, 위변조 차단을 효과적으로 수행할 수 있도록 하므로, 발생 가능한 여러 가지 위협으로부터 안전하게 콘텐츠를 사용할 수 있도록 하였다.



<그림 15> 구현 결과 화면

참 고 문 헌

[1] Zheng Yan, "Mobile Digital Rights Management", Nokia Research Center, 2001

[2] Gartner, "Digital Rights Management (DRM) Software: Perspective", 2002.

[3] Hideki Imai & Kazukuni Kobara, "Copyrights

Protection Techniques for the Future Network Society", Univ.of Tokyo
[4] OMA, "DRM Content FormatCandidate Version 1.0", OMA-Download DRMCF-v1_0-20030801-C, 2003.
[5] R.Vevers and C.Hibbert(2002), "COPY PROTECTION AND CONTENT MANAGEMENT IN THE DVB", KPMG Consulting(UK), 2002
[6] Bruce Schneuer, Applied Cryptography, Wiley, 1996.
[7] 이만영, 김지홍, 송유진, 염홍렬, 이임영 공저, "인터넷 보안 기술", 생능출판사, 2002.
[8] C.P. Pfleeger, "Security in Computing 2nd", Pretice Hall PTR, 2002.
[9] http://javadoc.iaik.tugraz.at/iaik_jce/current/iaik/security/cipher/TripleDES.html,iaik.security.cipher Class TripleDES

김 영 희 (Young-Hee Kim)

- 정회원
- 1993년 2월 : 순천향대학교 전산학과 (전산학 학사)
- 1997년 8월 : 순천향대학교 전산학과 (전산학 석사)
- 2005년 2월 : 성균관대학교 컴퓨터공학과 (컴퓨터공학 박사 수료)
- 2006년 11월 ~ 현재 : 백석대학교 정보통신학부, 그리스도대학교 경영정보학부 외래강사
- 관심분야 : 웹 마이닝, RFID 마이닝, DRM, 웹서비스

이 창 열 (Chang-Yeol Lee)

- 정회원
- 1985년 2월 : 고려대학교 수학과 (이학사)
- 1991년 2월 : 고려대학교 전산과학과 (이학석사)
- 1997년 6월 : University Paris VII
- 2000년 3월 ~ 현재 : 동의대학교 컴퓨터공학과 교수
- 관심분야 : 디지털 콘텐츠, 메타데이터, ID, RFID