안전하고 효율적인 콘텐츠 서비스 제공을 위한 CAS 적응형 DRM 모델의 설계 및 구현+

박성욱, 문종식, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail : [himtoss, comnik528, imylee]@sch.ac.kr

Design and Implementation of CAS adaptive DRM Model for Providing to Secure and Efficient Content Services

Sung-Wook Park, Jong-Sik Moon, Im-Yeong Lee
Department of Computer Software Engineering, Soonchunhyang University

요 약

지금의 IPTV는 IP기반 방송융합 서비스로서 현재 세계 유명 통신 사업자들을 중심으로 빠르게 발전하고 있다. 하지만 'IP+방송' 이라는 그저 단순한 결합과 부가서비스들의 제한으로 인해 기술의 비효율성이 드러나 있으며, 주로 IPTV서비스를 필두로 현재 콘텐츠에 대한 유출사고가 이루어지고 있다. 따라서 변화된 새로운 형태의 차세대 IPTV서비스와 더불어 그 특성에 맞게 보안 서비스에 대한 요구사항이 필요하다. 본 연구에서는 유무선 통합 환경에서 제공되는 IPTV서비스에서의 안전하고 효율적인 콘텐츠 서비스 제공을 위한 'CAS 적응형 DRM 모델'을 제안하였다. 사용자가 다운로드한 DRM이 적용된 콘텐츠를 안전하고 효율적으로 자신이 소유한 디바이스에서 이용할 수 있는 방안을 제시한다.

1. 서론

지금의 IPTV는 IP기반의 방송융합 서비스로서 현재 세계 유명 통신 사업자들을 중심으로 빠르게 발전하고 있다. 2009년 12월 KISA에서 진행한 국내 지식정보보안산업 시장 및 동향 조사 내용에 따르면 IPTV에 대한 투자규모가, 2008년에는 6,133억원, 2012년까지 5년간 총 1조 9천억원이 투자될 것으로 전망했고, 2009년 한국 IDC에서 발표한 국내 보안 소프트웨어 시장 조사 내용을 보면 2009년부터 2013년까지 급격하게 전체적인 보안 소프트웨어 시장이 증가하는 것을 볼 수 있다.[1][2] 이와 같이 현재 디지털 콘텐츠가 폭발적으로 증가하면서 그에 따른 콘텐츠에 대한 보안과 위협관리의 필요성이 요구되고 있다. 하지만 'IP + 방송' 이라는 그저 단순한 결합과 부가서비스들의 제한으로 인해 기술의 비효율성이 드러나 있으며, 2002년 3월에 시작하여 고주가를 달리던 위성 방송 서비스인 스카이라이프의 시장정체 현상과 같은 유사현상이 나타날 것으로 예상되고 있다. 또한 최근 콘텐츠의 유출사고가 주로 IPTV서비스를 필두로 이루어지고 있으며, 이용자들은 "시간과 장소에 구애받지 않고 다양한 환경에서 효율적으로 콘텐츠를 이용해야 한다." 는 다양한 소비욕구를 표출하고 있다. 지금의 IPTV서비스는 변화된 새로운 형태의 차세대 IPTV서비스와 더불어 그 특성에 맞게 보안 서비스에 대한 요구사항이 필요하다. 본 연구는 기존 IPTV서비스의 제한된 콘텐츠 이용을 해결하고자 각종 Personal Device와 연동을 통해 콘텐츠에 대한 활용도 및 효율성을 극대화시키고, 기존에 제공되던 보안 기술인 CAS(Conditional Access System)와 DRM(Digital Right Management) 각각의 특성을 살려 유무선 통합 환경에 제공되기 위한 'CAS 적응형 DRM 모델'을 구현하는 것이 본 연구의 목표이다.

+ 본 연구는 교육과학기술부와 한국산업기술재단의 지역혁신인력양성사업으로 수행된 연구결과임.

2. 관련연구

본 장에서는 기존 콘텐츠 보호를 위한 시스템인 CAS와 DRM에 대해 알아본다[3].

3.1 CAS(Conditional Access System)

CAS는 콘텐츠 보호를 위해 방송 시스템에 가입자(Subscriber)의 개념을 도입하여 수신자격(Entitlement)이 있는 시청자만 이 서비스를 이용 가능하도록 한 시스템이다. 수신자격이 없는 수신자는 시청이 불가능 하도록 데이터를 스크램블링 하는데 이때 방송 콘텐츠는 제어단어(CW: Control Word)를 이용하여 처리된다. 제어단어는 암호화되어 스크램블링 된 방송 데이터와 함께 전송되며 수신자는 암호화된 제어단어를 복호화하고 이를 이용해서 방송 데이터의 디스크램블링을 수행한다.

3.2 DRM(Digital Right Management)

DRM은 인터넷 환경에서 디지털 콘텐츠에 대한 생산

에서부터 디지털 콘텐츠의 전체 사이클에 걸쳐 지적 재산권을 관리하고 제어하기 위해 사용되는 기술이다. 디지털 콘텐츠의 데이터를 암호화하여 유통하고, 사용자 인증 및 단말기에 대해 라이선스를 발급함으로써 콘텐츠의 불법 복제를 방지할 수 있다. DRM 시스템은 디지털 콘텐츠를 암호화하는 DRM 패키저와 라이선스를 발급 및 관리하는 클리어링 하우스, 발급받은 라이선스를 이용하여 사용하는 DRM 클라이언트로 구성되어 있다. 라이선스는 콘텐츠에 대한 사용권한과 복호화 키를 포함하고 있는데, 사용 권한에 대한 제한 조건과 비교하여 조건에 맞는 경우에만 복호화를 수행할 수 있도록 하였다.

3. 보안요구사항

본 연구에서 제안하고자 하는 방식은 사용자가 다운로드한 콘텐츠를 자신이 소유한 디바이스에 안전하고 효율적으로 전달하기 위한 것을 목적으로 다음과 같은 요구사항을 가진다[4].

- 기밀성 : 서비스를 위해 통신에 사용되는 데이터는 정당한 개체만이 확인할 수 있어야 한다. 기밀성은 정보를 해석할 수 없도록 암호화를 통해서 이루어진다.
- 무결성 : 서비스에 필요한 저장 데이터와 네트워크를 통해 전송되는 데이터가 위/변조 되거나 파괴되지 않도록 해야 한다. 만약 위조, 삭제 및 변조가 되었다면 그 사실을 확인할 수 있어야 한다.
- 인증 : 정당한 사용자만이 서비스를 이용할 수 있도록 인증이 이루어져야 한다. 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 접근제어 : 정보 자원에 대한 읽기나 변경 등의 모든 접근 행위에 대해 그 권한을 명백히 구분해 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다.

4. 제안방식

본 연구에서는 CAS와 DRM 연동을 통해 제한된 다운로드 콘텐츠를 사용자 디바이스에서도 자유롭게 이용할 수 있는 방법을 제안한다.

4.1 시스템 계수

다음은 본 제안 방식에서 사용되는 시스템 계수이다.

- $*$: 참여 객체(S : Server, C : Client)
- uid : 사용자의 아이디
- $pass$: 사용자의 패스워드
- CW : Control Word(스크램블 시 사용)
- EMM : 자격 관리 메시지
- ECM : 자격 제어 메시지
- AK : ECM의 암호 키(인증 키)
- DK : EMM의 암호 키(분배 키)
- K_* : $*$의 세션 키
- KR_* : $*$의 개인 키
- KU_* : $*$의 공개 키
- K_V : CP와 키관리 서버 간 세션키
- K_P : 컨텐츠 패키징 키
- K_S : 홈게이트웨이와 키관리서버 간 세션키
- CR : 콘텐츠 사용규칙
- CN : 콘텐츠 식별번호

4.2 세션 키 동기화 단계

키 동기화 단계는 Client가 Server에 접속 요청할 시에 이루어지는 단계로 과정은 다음과 같다.

Step 1. Client가 Key Management Server의 공개 키를 요청한다.

Step 2. Key Management Server는 Client에게 자신의 공개 키를 전송한다.

Step 3. Client는 세션 키 K를 생성하여 Key Management Server의 공개 키로 암호화 하여 Key Management Server로 전송한다.

$$E_{KU_s}[K]$$

Step 4. Key Management Server는 자신의 개인 키로 $E_{KU_s}[K]$를 복호화 한 후 세션 키 K를 획득한 후에 세션 키 K를 K로 암호화 하여 Client에 전송함으로써 키 동기화가 완료된다.

$$D_{KR_s}[E_{KU_s}[K]]$$
$$E_K[K]$$

4.3 신규 가입 단계

신규 사용자 등록 단계는 사용자가 Key Management Server에 사용자 개인정보를 저장하는 단계이다.

Step 1. 사용자는 회원가입 정보를 세션 키 K로 암호화한 후 Key Management Server로 전송한다.

(가입정보=ID||비밀번호||이름||연락처||서비스등급)

Step 2. Key Management Server는 전송받은 데이터를 바탕으로 회원 등록을 처리한다.

4.4 사용자 인증 단계

인증 단계는 사용자로부터 ID, Password를 입력받아 Key Management Server에서 검증하는 단계이다.

Step 1. Client는 사용자에게 uid, pass를 요청한다.

Step 2. Client는 입력받은 정보를 세션 키 K로 암호화한

후 Key Management Server에 전송한다.

$E_K[uid||pass]$

Step 3. Key Management Server 전송받은 사용자 정보를 바탕으로 검증 후에 인증 정보가 담긴 Auth를 발급한 후 세션 키 K로 암호화한 후 Client에 전송한다.

$D_K[E_K[uid||pass]]$

$E_K[Auth]$

4.5 콘텐츠 패키징 키 생성 및 콘텐츠 패키징 단계

키 생성 및 패키징 단계는 해당 콘텐츠에 대응되는 패키징 키 생성과 패키징 키를 통해 콘텐츠를 패키징화 하는 단계이다.

Step 1. Content Provider는 패키징이 필요한 콘텐츠의 대한 정보를 세션 키 K로 암호화 하여 Key Management Server로 전송한다.

$E_K[ContentInfo]$

$ContentInfo = [Creator||CN||Title||DSIG]$

Step 2. Key Management Server는 전송받은 Content Info를 복호화한 후 패키징 키 생성기를 통해 K_P를 생성하고 세션 키 K로 암호화하여 Content Provider로 전송한다.

$E_K[K_P]$

Step 3. Key Management Server 전송받은 패키징 키를 콘텐츠 패키저를 통해 패키징된 콘텐츠를 생성하여 Content Server로 전송한다.

$E_{K_P}[CR||URL||CN||E_{K_P}[Content]]$

4.6 Content Server와 Client 간 콘텐츠 다운로드 단계

콘텐츠 다운로드 단계는 Client가 Content Server로 부터 패키징 콘텐츠를 획득하는 단계로 과정은 다음과 같다.

Step 1. Client는 콘텐츠 다운로드 요청 시 필요한 Payment Info와 Key Management Server와의 세션 키 K_S로 암호화된 Request Info를 Content Server 세션 키 K_C로 다시 암호화 하여 Content Server로 전송한다.

$PaymentInfo = [MSG(OK \text{ or } Failed)||CN]$

$E_{K_C}[PaymentInfo||E_{K_S}[RequestInfo]]$

$RequestInfo = [CN||CR||uid]$

$E_K[RequestInfo]$

Step 2. Content Server는 Payment Info 획득 후 결재정보 검증과 Content 식별번호 확인을 통해 대응되는 패키징 콘텐츠를 Client로 전송하고, 콘텐츠 요청정보를 키관리서버로 전송한다.

$E_{K_P}[CR||URL||CN||E_{K_P}[Content]]$

4.7 라이선스 생성 · 발급 및 콘텐츠 언패키징 단계

다음 단계는 다운로드 받은 패키징 콘텐츠 이용을 위한 라이선스 생성,발급 및 해당 콘텐츠의 언패키징 단계로 과정은 다음과 같다.

Step 1. 앞서 설명한 단계의 과정을 통해 로그인 후 Client는 해당콘텐츠에 대한 요청정보를 K_S로 암호화 후 Key Management Server로 전송한다.

$RequestInfo = [CN||CR||uid]$

$E_K[RequestInfo]$

Step 2. Key Management Server는 콘텐츠 요청정보를 획득 후 사전에 Content Server로부터 받은 요청정보와 비교 검증 후 라이선스를 생성하여 Client에게 전송한다.

$License = [uid||K_P||CR||CN||dev]$

$E_{K_s}[License]$

4.8 클라이언트와 디바이스 간 인증 및 키 동기화 단계

인증 및 키 동기화 단계는 클라이언트와 디바이스간의 접근 시 요청을 수락하기 위한 단계로 그 과정은 다음과 같다.

Step 1. 세션 키 동기화 과정을 거친 후 디바이스는 기존 클라이언트와 Key Management Server간 사용되던 uid, pass 정보를 K_g로 암호화 후 Client로 전송한다.

$E_{K_s}[uid||pass]$

Step 2. Client는 uid, pass를 획득, 검증 과정을 거친 뒤 디바이스정보를 Client에 등록한다. 그 후에 스트리밍에 사용될 분배 키 DK를 생성 후 K_g로 암호화 후 디바이스로 전송한다.

$D_{K_s}[E_{K_s}[uid||pass]]$

$E_{K_g}[DK]$

5.9 스트리밍 콘텐츠 제공 단계

스트리밍 콘텐츠 제공 단계는 디바이스가 요청한 해당 콘텐츠를 Client가 스트리밍 형태로 제공해주는 단계이다.

Step 1. 디바이스는 분배 키 DK로 Content 식별번호와 디바이스 정보를 암호화하여 전송한다.

$E_{DK}[CN||Dev]$

Step 2. Client는 Content 식별번호와 디바이스 정보 검증 후 요청한 콘텐츠에 대한 스크램블 과정을 거친 후 디바이스로 전송한다.

$E_{DK}[EMM||ECM||ScrambleData]$

$EMM = D_{DK}[E_{DK}[\text{사용권한}||AK]]$

$ECM = D_{AK}[E_{AK}[\text{제어변수}||CW]]$

$ScrambleData = D_{CW}[E_{CW}[ContentData]]$

5. 제안방식 구현

4장에서 설계한 내용을 기반으로 안전하고 효율적인 CAS 적응형 DRM 모델을 구현하였다.

5.1 서버 및 스트리밍 서버

그림 1과 그림 2를 통해 알 수 있듯 서버에서는 전반적인 통신 현황을 알 수 있으며, 콘텐츠 암호화, 스트리밍 등록 등의 기능을 수행한다.

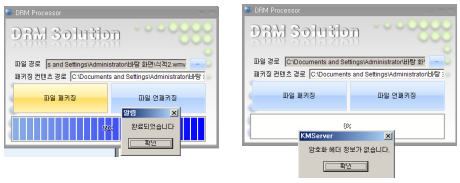
스트리밍 서버는 클라이언트의 콘텐츠 요청정보를 받아 해당 콘텐츠를 전송해주고 스트리밍 서비스 제공 역할을 수행한다.

5.2 클라이언트 및 디바이스 클라이언트

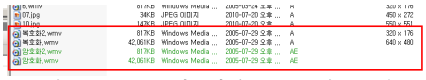
그림 4, 그림 5와 같이 클라이언트는 콘텐츠 스트리밍 서비스, 라이센스 발급, 콘텐츠 다운로드 및 다양한 부가 서비스를 이용 기능을 수행한다.

디바이스 클라이언트는 클라이언트로부터 스트리밍 서비스를 받는 역할을 수행한다.

(그림 1) 서버 로그 정보 화면



(그림 2) 콘텐츠 패키징 및 헤더 정보 판별



(그림 3) DRM이 적용된 콘텐츠 정보

(그림 4) 인증 후 스트리밍 서비스 이용 화면

(그림 5) 라이선스 발급 화면

(그림 6) 암호화된 라이선스 정보

6. 제안방식 분석

본 제안 방식에서는 대칭키 암호알고리즘(DES, AES)와 공개키 암호알고리즘(RSA)을 사용함으로써 기본적인 보안 요소를 제공하고 있다.

- 기밀성 : 주된 통신에 사용될 세션 키는 공개 키로 암호화하여 전송되기 때문에 통신로 상에서의 불법적인 도청 및 공격으로부터 안전하여 기밀성이 보장된다. 이후 통신도 세션 키를 통해 이루어지므로 기밀성을 보장한다.
- 무결성 : 분배된 세션 키를 통해 주고 받는 메시지는 위변조로부터 안전하며, 이에 대한 검증을 할 수 있다.
- 인증 : 정당한 사용자만이 라이선스 및 스트리밍 서비스를 이용할 수 있도록 디바이스 및 사용자 인증이 이루어지며 인가되지 않은 사용자는 서비스를 이용할 수 없다.
- 접근제어 : 라이선스를 저장된 정보를 통해 콘텐츠가 암호화되어져 있기 때문에 서비스 이용은 정당한 사용자만이 가능하고 이를 이용해 디바이스 스트리밍 서비스 또한 접근을 제어가 가능하다.

7. 결론

본 연구는 CAS 적응형 DRM 모델을 통해 유무선 통합 IPTV환경에서 안전하고 효율적인 콘텐츠를 제공이 가능하다. 즉, 기존 서비스에서의 문제점인 콘텐츠에 대한 '제약성'과 '활용도' 부분이 크게 개선되어 사용자에게 4A(Any time, Any where, Any device, Any Content)환경을 제공할 수 있으며, 디바이스형태에 맞는 상이한 콘텐츠를 일일이 다운 받지 않고 스트리밍 서비스형태로 제공함으로서 효율적인 콘텐츠 서비스를 제공받을 수 있다. 또한 사업자 측면에서 콘텐츠에 대한 컨버트 및 스트리밍 서버가 사용자의 홈게이트웨이에서 진행되므로 장기적으로 보았을 때 네트워크 비용 절감 효과를 기대할 수 있다. 마지막으로 콘텐츠 보안 기술인 DRM과 CAS 연동을 통해 보다 효율적이고 안전한 콘텐츠 제공이 가능할 것으로 기대된다.

참고문헌

[1] 고순주, 박영준, "미디어 융합과 IPTV 정책 및 시장동향", 전자통신동향분석 제 23권 제2호, pp105, 2008. 4

[2] 이정열, 정길원, "2009 국내 지식정보보안산업 시장 및 동향 조사", 한국인터넷진흥원, 2009

[3] 윤기송, "CAS-DRM 연동기술", TTA Journal No.117, pp120-122, 2008

[4] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신보안 3rd Edition", 도서출판 그린, 2005. 8. 20.