IPTV에서 멀티미디어 서비스 제공을 위해 OTP를 이용한 가입자 인증기술+

문종식, 이임영
순천향대학교 컴퓨터학부
e-mail:comnik528@sch.ac.kr

Subscriber Authentication Technology using OTP for Multimedia Service Offer in IPTV

Jong-Sik Moon, Im-Yeong Lee
Division of Computer Science and Engineering, Soonchunhyang University

요 약

현대사회는 IT 기술의 급속한 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 인해 u-지식사회라는 새로운 문화적 변환기를 맞이하고 있다. 특히 광대역 통합망 환경이 구축되면 방송의 IPTV와 통신의 VoIP 서비스는 많은 수요를 불러올 것으로 예상된다. 그러나 IPTV를 제공받는데 있어 불법적인 개인정보 수집, 기술적 개인정보 유출됨에 따라 무분별하게 불법제어, 콘텐츠 불법 유통, 서비스 도용, 비인가자 접근 등의 문제점이 발생할 수 있다. 따라서 본 연구에서는 멀티미디어 서비스 제공을 위한 가입자 인증 기술에 관한 연구를 진행하여 멀티미디어 서비스를 제공하는데 있어 가입자 측면에서의 안전성과 효율성을 제공하도록 하였다.

1. 서론

현대사회는 IT 기술의 급속한 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 인해 u-지식사회라는 새로운 문화적 변환기를 맞이하고 있다. 앞으로는 콘텐츠, 네트워크 및 단말 분야에서 디지털 컨버전스 현상이 급진전되어 기존 통신과 방송의 경계가 허물어질 것이다. 대통합 현상이 빠르게 진전되어 지능화, 융·복합화, 광대역화가 사회전반으로 확산되고 모든 정보단말, 가전기기, 사물 등이 하나의 네트워크에 연결되는 광대역통합망 기반의 네트워크사회(Broadband Network Society)로 빠르게 진화될 전망이다. 이와 같은 변화는 현대 사회에서 디지털화의 가속 및 통신 인프라의 확충 등으로 인해 IP 네트워크로 연결되어 영상 및 음성 정보를 서로 공유할 수 있는 환경이 제공 되고 통합 서비스에 대한 수요가 증가하고 있다. 따라서 방송과 통신의 융합 흐름은 더욱 가속화될 전망을 보이고 있으며, 특히 광대역 통합망 환경이 구축되면 방송의 IPTV(Internet Protocol TV)와 통신의 VoIP(Voice over IP) 서비스는 많은 수요를 불러올 것으로 예상된다. 차세대 융합 서비스는 디바이스의 다양성과 디지털 정보의 공유 등으로 보안 요구사항은 더욱 다양해지며, 기존 IP 네트워크 기반으로 차세대 융합서비스를 제공할 경우 이전의 사이버공격 기술이 그대로 적용될 수 있는 문제점을 가지고 있다. 즉, IP 네트워크를 통해 IPTV를 제공받는데 있어 쿠키에 의한 개인정보 수집, 해킹·악성코드 등 불법적인 개인정보 수집, 바이러스 등에 의한 기술적 개인정보 유출, IP 망을 통한 광고 안내 및 구매 권유 등이 가능하며, 사용자가 리모트 컨트롤을 사용하여 채널을 돌리거나 물건을 구매하는 등의 조작 행위 정보가 제 3자의 해킹에 노출될 우려가 있다. 또한 방송사업자가 아닌 개인도 자체 방송서비스를 제공할 수 있는 환경이 조성됨에 따라 무분별하게 타인의 동의 없이 사생활을 촬영·방송하는 등 불법제어, 콘텐츠 불법 유통, 서비스 도용, 비인가자 접근 등의 문제점이 발생할 수 있다[1][2][6]. 이러한 여러 취약점이 존재함에 따라 본 연구에서는 멀티미디어 서비스 제공을 위한 가입자 인증 기술에 관한 연구를 진행하였다. 본 논문의 구성은 다음과 같다. 2장에서는 연구 배경으로 IPTV 보안 기술 및 보안 요구 사항에 대하여 기술하고 3장에서는 기존 연구에 대하여 분석한다. 4장에서는 안전하고 효율적인 가입자 인증 기술을 제안하고, 5장에서는 제안 방식을 분석하여 마지막으로 6장에서는 결론 및 향후 연구 방향을 서술한다.

+ 본 연구는 교육과학기술부와 한국산업기술재단의 지역혁신인력양성사업으로 수행된 연구결과임

2. 연구 배경

본 장에서는 IPTV 보안 기술의 개요에 대하여 알아보고, 일반적인 IPTV 상에서 일어날 수 있는 보안 요구 사항에 대하여 분석하고자 한다.

2.1 IPTV 보안 기술

기존에 가장 대표적인 IPTV 보안 기술로 CAS와

DRM의 개요에 대하여 알아보고 각 방식별 특징 및 장/단점을 분석한다.

가. 방송 수신제한시스템(CAS)

CAS(Conditional Access System)는 과거 아날로그 방송 시절부터 유료 방송 서비스를 위해 방송 서비스에 대한 고객의 접근 여부를 제어하는 기본 시스템으로 사용되어 왔다. CAS는 기존 방송 서비스에서 사용해 왔던 콘텐츠 보안 솔루션이란 측면에서 많은 방송 사업자들에게 신뢰를 얻고 있는 솔루션이지만 IPTV 서비스에 적용된 CAS는 여러 문제점을 나타내고 있다. 이는 처음에 단방향 방송에 적합한 구조를 바탕으로 도입된 CAS의 태생적인 문제 때문이다. CAS의 내재적인 문제점 이외에도 CAS는 콘텐츠의 전송 통로에 대한 접근 제어 솔루션이라는 점에서 IP 네트워크 환경 하의 순수 VOD 나 PVR 등의 기능에 직접적으로 대응하기 어렵다는 문제점을 가지고 있다. 저장된 콘텐츠를 지속적으로 관리할 수 있는 안전한 키 관리와 VOD를 포함한 다양한 서비스에 대한 결제 방식 및 권한 제어 문제가 IPTV 서비스 보안에 있어 CAS의 문제점이다[5].

나. 디지털저작권관리(DRM)

DRM(Digital Right Management)은 인터넷 환경에서 디지털 콘텐츠에 대한 지적재산권을 관리하고 제어하기 위해 주로 사용되는 기술이다. 불법 복제를 방지하기 위하여 디지털 콘텐츠의 데이터를 암호화하여 유통하고, 인증된 사용자 및 단말기에 대해서만 라이센스를 발급함으로써 콘텐츠의 이용을 제어한다. DRM은 인터넷 및 PC 기반의 콘텐츠 유통 환경에 적합하게 발전된 기술이므로 기본적으로 IPTV 서비스에 적합한 콘텐츠 보호 기술이다. 다만, 라이센스 발급 요청을 하기 위한 회귀 경로(Return Path)가 없는 경우에는 DRM도 CAS와 마찬가지로 ECM / EMM 기능이 반드시 필요하다[5].

2.2 보안 요구 사항

IPTV에서의 보안 요구사항은 다음과 같다.

가. 보안 요구 사항

- 기밀성 : 멀티미디어 서비스를 제공하는데 있어 전송되는 멀티미디어 데이터 및 사용자 개인정보 등 제 3자의 공격으로부터 안전해야 한다.
- 무결성 : 멀티미디어 서비스를 위해 전송되는 데이터가 위/변조 되거나 파괴되지 않도록 해야 한다. 만약 위조, 삭제 및 변조가 되었다면 그 사실을 확인할 수 있어야 한다.
- 인증 : 서비스를 이용하고자 접근하는 사용자가 정당한 권한을 가지고 접근하려는 것인지 검증할 수 있어야 한다.
- 접근제어 : 정당하게 인증을 받지 않은 사용자는 서비스에 접근하지 못해야 하며, 서비스를 제공받을 수 없어야 한다.
- 개인정보 유출 : 공격자의 불법적인 접근에 의한 사용자의 식별 정보 및 인증 정보 등 개인정보 유출로부터 안전하게 보호되어야 한다.
- 신분위장 : 멀티미디어 서비스를 제공받기 위해 정당한 사용자로 위장하여 서비스에 접근하거나 인증을 받을 수 없어야 한다. 이에 제 3자가 정당한 가입자처럼 접근하는 것에 대한 안전성을 제공해야한다.
- 세션 하이재킹 : 하이재킹을 통해 세션을 훔치는 것뿐만 아니라 서버와 사용자가 주고받는 모든 정보를 도청할 수도 있기 때문에 네트워크 및 데이터에 대한 안전성을 유지해야 한다.

3. 기존 연구

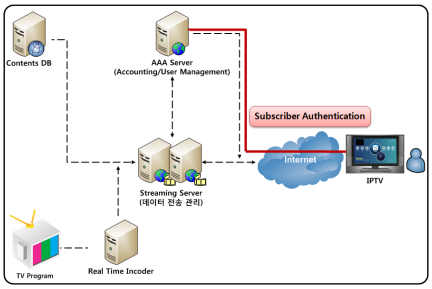
기존에 연구된 멀티미디어 서비스에서의 인증 방식의 개요에 대하여 알아보고 각 방식별 특징 및 장/단점을 분석한다.

3.1 IMS/SIP펨토셀 환경 내에 IPTV 컨텐츠 보안을 위한 인증 기법

최근 정보통신부가 발표한 IT839 전략에 따르면, 향후 방송과 통신의 융합 흐름은 더욱 더 진보될 전망이며, IPTV 서비스는 더 많은 수요를 불러올 것으로 예상되는데, 성공적인 사업화와 서비스 활성화를 위해서는 컨텐츠 서비스 보안이 절실히 요구되고 있다. 이 방식에서는 컨텐츠 불법유통을 막고자 IMS/SIP펨토셀 환경 내에 3세대 IPTV의 컨텐츠 보안을 위한 인증기법 설계에 대해 제시하였으며, 가입 펨토셀존에서는 모든 영상 디바이스는 IPTV서비스를 지원 받고, 그 외 범주일시(가입안한 펨토셀존 포함)에는 IPTV서비스를 차단하도록 설계하였다[4]. 그러나 사용자 인증 방식과 디바이스 인증 방식을 통한 인증을 제공하나 1차원적인 인증 방식을 이용하기 때문에 보안상 매우 취약하며, 디바이스와 사용자 인증단계를 거치기 때문에 서비스를 이용하는 사용자의 불편함을 초래하는 문제점을 지니고 있다.

3.2 Single-Sign-On을 이용한 사용자 인증 방식

Single-Sign-On은 사용자가 단한번의 인증을 통하여 추가적으로 인증할 필요가 있는 다른 서비스로의 자동적인 인증을 제공한다. 다수의 사용자가 다수의 서비스를 제공받기를 원하는 IPTV환경에서는 단순한 사용자 인증과 접근제어의 기능을 가진 제한수신시스템과 빈번한 사용자 인증의 번거로움을 해결할 수 있는 편의성을 제공하는 SSO의 융합은 필연적임에 따라 이 방식에서는 제한수신시스템과 SSO의 기능을 통합하여 IPTV환경에 적합한 새로운 인증방안을 제안하였다[3]. 그러나 Kerberos 방식과의 큰 차이점이 없으며, IPTV에 SSO를 적용하기에는 콘텐츠를 제공하는 서비스의 분산형태가 아니기 때문에 적합하지 않다는 문제점이 있다.



(그림 1) IPTV에서 가입자 측면의 보안 개념도

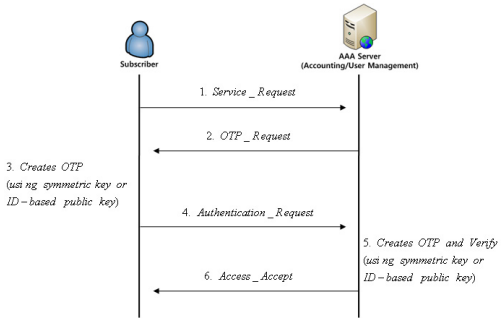
4. 가입자 인증 기술

제안 방식은 (그림 1)과 같이 IPTV 전체 개념도에서 인증 서버와 가입자 측면에서의 멀티미디어 서비스 제공을 위해 OTP를 이용한 가입자 인증 기술을 제안하였다. 가입자는 서비스를 제공받기위해 OTP를 이용하여 인증을 받으며, 정당한 사용자는 서비스를 제공받을 수 있다. 인증을 위한 수단으로 사용되는 OTP를 대칭키와 ID 기반 공개키를 이용하는 방식으로 제안하였다.

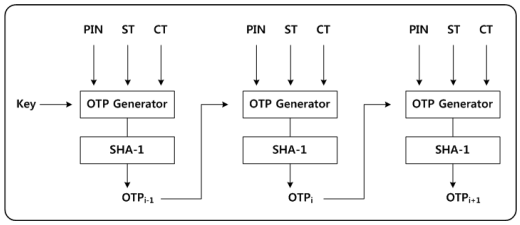
4.1 시스템 계수

가입자 인증 기술에서 사용되는 시스템 계수는 다음과 같다.

- $*$: 각각의 개체(S : 가입자, $AAAS$: 인증 서버)
- ID_* : $*$의 아이디
- OTP : 일회용 패스워드
- PIN : 가입자 단말기의 일련번호
- ST : OTP 입력 값으로 동기화 되어있는 시간 값
- CT : OTP 입력 값으로 동기화 되어있는 카운터
- g : 곱셈군 Z_n^*의 생성자
- $h()$: 안전한 일방향 해쉬 함수
- e : $G_1 \times G_1 \rightarrow G_2$ 겹선형 사상
- $E_*[\,]$: $*$의 키로 암호화
- KS : 가입자와 인증 서버가 사전에 공유한 대칭키
- KU_*/KR_* : $*$의 ID 기반 공개키/개인키



(그림 2) 가입자 인증 프로토콜 흐름도



(그림 3) 대칭키를 이용한 OTP 방식

4.2 가입자 인증 프로토콜

가입자 인증 프로토콜은 대칭키를 이용한 OTP 방식과 ID 기반 공개키를 이용한 OTP 방식으로 구성되며, 각각의 방식은 개별적인 제안 프로토콜이다. 두 방식의 인증 프로토콜은 인증 수행 시 프로토콜은 동일하며 인증을 받는 인자를 대칭키 및 공개키를 이용한 방식으로 제안하였다. 대칭키 KS는 사전에 가입자 등록 시 분배되었다고 가정한다.

가. 대칭키를 이용한 OTP 방식

대칭키를 이용한 OTP 방식은 가입자와 인증 서버가 OTP를 생성하는데 사용되는 입력 값은 (그림 3)과 같이 모두 4개이며, 출력된 값은 SHA-1를 거쳐 최종 출력 값이 인증을 위해 사용되는 OTP 값이다. 이전 단계에서 생성된 OTP는 다음 단계에 생성될 OTP의 키 값으로 사용된다.

Step 1. 가입자가 서비스를 이용하고자 할 때 디바이스는 OTP를 생성한다.

$$OTP_{i-1} = h(PIN \oplus ST \oplus CT \oplus Key)$$

Step 2. 세션이 종료하고 다음 세션에서 서비스를 이용할 때 생성되는 OTP는 이전 세션에서 사용한 OTP를 키 값으로 입력받아 생성한다.

$$OTP_i = h(PIN \oplus ST \oplus CT \oplus OTP_{i-1})$$

나. ID 기반 공개키를 이용한 OTP 방식

ID 기반 공개키를 이용한 OTP 방식은 OTP를 생성하는데 있어 겹선형 사상을 이용하여 생성한다.

Step 1. 가입자와 인증 서버는 자신의 ID 기반 공개키/대칭키 쌍을 생성한다.

$$KU_S = ID_S,\ KR_S = ID_S \bullet g^{KS}$$

$$KU_{AAAS} = ID_{AAAS},\ KR_{AAAS} = ID_{AAAS} \bullet g^{KS}$$

Step 2. 가입자는 서비스를 이용하고자 할 때 자신의 ID 기반 개인키와 사전에 공유한 대칭키 그리고 인증 서버의 ID 기반 공개키를 이용하여 OTP를 생성한다. OTP를 생성할 때 겹선형 사상을 기반으로 하여 생성한다.

$$OTP = e(KR_S,\ KS \bullet KU_{AAAS})$$

Step 3. 인증 서버는 OTP를 검증할 때 자신의 ID 기반 개인키와 가입자의 공개키 그리고 사전에 공유한 대칭키를 이용하여 OTP′를 생성하여 전송된 OTP와 비교하여 검증한다.

$$OTP' = e(KR_{AAAH},\ KS \bullet KU_S)$$
$$OTP' \stackrel{?}{=} OTP$$

5. 제안 방식 분석

제안 방식을 2.2절에서 언급한 보안 요구사항에 맞추어 분석하면 다음과 같다.

- 기밀성 : 전송되는 개인정보 데이터 및 인증정보는 OTP 방식에 따라 대칭키와 ID 기반 공개키를 이용하여 안전하게 보호할 수 있다.
- 무결성 : 인증을 위해 사용되는 OTP 인자는 대칭키를 이용한 방식에서는 SHA-1을 이용하여 무결성을 제공할 수 있으며, ID 기반 공개키를 이용하는 방식에서는 겹선형 사상을 기반으로 OTP를 설립하기 때문에 무결성을 제공할 수 있다.
- 인증 : 서비스를 이용하고자 접근하는 사용자가 정당한 권한을 가지고 접근하려는 것인지 검증하기 위해 두가지 방식의 OTP를 제안하였으며, 기존의 CAS 및 STB에 키를 저장하여 인증 받는 방식보다 안전성을 높일 수 있다.
- 접근제어 : 불법적인 접근을 통해 서비스를 이용하고자 하는 사용자는 인증을 제공받지 못하기 때문에 서비스를 이용할 수 없다.
- 개인정보 유출 : 공격자는 인증 서버에 불법적인 접근 및 도청을 할 수 없기 때문에 개인정보의 유출로부터 안전하게 보호할 수 있다.
- 신분위장 : OTP를 이용하여 인증을 제공하고 있기 때문에 도청 및 재전송 공격으로부터 안전하며, OTP를 생성함에 있어 이전 세션 OTP를 입력 값으로 사용하기 때문에 정당하지 않은 사용자는 서비스를 이용할 수 없다.
- 세션 하이재킹 : 네트워크 및 데이터에 대한 안전성은 대칭키와 ID 기반 공개키를 이용하여 안전성을 제공할 수 있으며, 세션을 훔치더라도 OTP의 사용 및 이전 세션의 OTP와 동기화 값들을 이용하여 인증 정보를 생성하기 때문에 하이재킹 공격으로부터 안전하다.

6. 결론

IT 기술의 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 디지털 컨버전스 현상이 급진전되어 기존 통신과 방송의 경계가 허물어질 것으로 전망되며, IPTV와 통신의 VoIP 서비스는 많은 수요를 불러올 것으로 예상된다. 차세대 융합 서비스는 디바이스의 다양성과 디지털 정보의 공유 등으로 보안 요구사항은 더욱 다양해지며, 기존 IP 네트워크 기반으로 차세대 융합서비스를 제공할 경우 이전의 사이버공격 기술이 그대로 적용될 수 있는 문제점을 가지고 있다. 이러한 여러 취약점이 존재함에 따라 안전하고 효율적인 멀티미디어 서비스 제공을 위해 OTP를 이용한 가입자 인증 기술을 제안하였다. 가입자는 서비스를 제공받기위해 OTP를 이용하여 인증을 받으며, 정당한 사용자는 서비스를 제공받을 수 있다. 인증을 위한 수단으로 사용되는 OTP를 대칭키와 ID 기반 공개키를 이용하는 방식으로 제안하였다. 대칭키를 이용하는 OTP방식은 카운터와 시간을 이용하여 생성하며, ID 기반 공개키를 이용하는 방식은 겹선형 사상을 기반으로 하여 OTP를 생성한다. 이를 통해 기존의 CAS 및 STB에 키를 저장하여 사용하는 방식보다 안전성과 효율성을 제공할 수 있다. 향후 가입자의 권한 및 과금에 관한 연구와 네트워크 측면과 서비스 제공자 측면에서의 보안기술 개발이 필요할 것으로 사료된다.

참고문헌

[1] Adi Shamir, “Identity-based cryptosystems and signature schemes,” CRYPTO′84, pp.47-53, 1984.

[2] Yang Xiao, Xiaojiang Du, Jingyuan Zhang, Fei Hu, Sghaier Guizani, “Internet Protocol Television: The Killer Application for the Next-Generation Internet,” IEEE Communication Magazine, pp.126-134, 2007.

[3] 김 강 ,정종일, 송상훈, 신동규, 신동일, “Single-Sign-On을 이용한 IPTV 사용자 인증방안,” 2006년도 한국정보과학회 가을 학술발표논문집, Vol. 33, No. 2(C), pp. 540-543, 2006.

[4] 김주용, 조인석, 김학춘, 이병관, “IMS/SIP펨토셀 환경 내에 3세대 IPTV의 컨텐츠 보안을 위한 인증기법 설계,” 한국인터넷정보학회 춘계학술발표대회. 제9권 제1호, pp. 155-159, 2008.

[5] 우제학, 노창현, 이완복, “IPTV 콘텐츠 보호 기술의 비교,” 한국콘텐츠학회논문지 Vol. 6, No. 8, pp. 157-164, 2006.

[6] 이철수, 박석천, “IPTV의 프라이버시 침해요인 분석 및 보호방안 연구,” 한국정보보호진흥원 최종연구보고서, 2007.