Open IPTV 환경에서의 사용자 인증 및 키 분배

정지연, 도인실, 채기준
이화여자대학교 컴퓨터공학과
e-mail : jemini1230@naver.com

User Authentication and Key Distribution in Open IPTV

Jiyeon Jung, Insil Doh, Kijoon Chae
Dept. of Computer Science & Engineering, Ewha Womans University

요 약

IPTV 는 대표적인 방송통신융합 산업으로 IT 망의 양방향성을 이용한 서비스의 차별화를 내세우며 여러 사업자에 의해 서비스가 이루어지고 있다. 기존 유선 통신망을 중심으로 제공되어 왔던 IPTV 서비스는 최근 모바일 환경 등으로 그 영역을 확대하기 위해 연구가 진행되고 있으며, 다른 한편으로는 IPTV 서비스를 위한 플랫폼 등을 개방하여 사업자가 아닌 일반인도 IPTV 를 통한 방송을 할 수 있는 구조인 Open IPTV 에 대한 연구가 활발하다. 이러한 Open IPTV 환경에서는 다수의 컨텐츠 제공자가 존재하기 때문에 기존 IPTV 에서 사용 되는 특정 기기 혹은 스마트카드를 통한 사용자 인증 및 키 분배가 어려운 실정이다. 따라서 본 논문에서는 Open IPTV 환경에서 안전한 컨텐츠 전송을 위한 사용자 인증 및 키 분배 시스템을 제안하고자 한다.

1. 서론

최근 IPTV 는 미디어 서비스 업계에서 새로운 사업 모델로서 주목 받고 있다. 업계에서는 IPTV 사업의 성공을 위해서는 단순히 IP 망을 이용한 방송서비스에 그치는 것이 아니라 IP 망의 양방향성을 이용한 대화형의 개인화 된 서비스를 제공해야 한다는 것에 의견을 모으고 있다.

위와 같은 IPTV 의 차별화 된 발전을 위하여 학계에서는 Open IPTV 라는 개념을 정의하고 Open IPTV Solution 의 표준화를 진행하고 있다. 주요 표준화 단체로는 Open IPTV Forum 이 존재하며, 이 단체는 managed, 혹은 non-managed network 상에서의 개인화 된 IPTV 서비스를 제공하기 위한 End-to-End Solution 을 개발하는 것을 목표로 하고 있다 [1].

Open IPTV 는 IPTV 의 서비스 플랫폼을 공개적으로 개방함으로써 특정 IPTV 서비스 제공자나 네트워크 망 사업자, 단말기 사업자 등에 얽매이지 않고 궁극적으로는 일반인도 IPTV 서비스를 할 수 있는 환경을 말한다. 또한 기존 단말기나 스마트카드 등을 이용한 가정 단위의 사용자 인증이 아닌 사용자 개별적인 인증을 통해 개인화 된 서비스를 제공해야 한다. 이와 같은 환경에서는 기존에 IPTV 서비스에 이용되어 왔던 스마트카드 및 단말기를 이용한 사용자 인증 및 키 분배는 더 이상 적합하지 않으며, Open IPTV 환경을 위한 새로운 메커니즘을 필요로 한다 [2].

이에 따라 본 논문에서는 Open IPTV 환경에서 안전한 컨텐츠 전송을 위한 사용자 인증 및 키 분배 시스템을 제안한다. 본 논문의 구성은 다음과 같다. 2 장에서는 제안 시스템의 관련 연구에 대하여 소개하고 3 장에서는 제안하는 시스템을 기술하며 마지막으로 4 장의 결론 및 향후 연구방향으로 논문을 마무리하도록 한다.

2. 관련 연구

본 논문에서는 기존 분산 네트워크에서의 인증 메커니즘인 Kerberos 와 기존 IPTV 에 사용되는 컨텐츠 보호 기술인 CAS 를 바탕으로 Open IPTV 환경에 맞는 사용자 인증 및 키 분배 메커니즘을 제안 하였다.

2.1. Kerberos [3]

Kerberos 는 오픈 된 네트워크 환경에서 신뢰 받는 제 3 자를 통한 서버와 클라이언트 간의 인증 프로토콜을 말하며 MIT 에서 진행 된 Project Athena 에 의해 개발되었다.

Kerberos 의 원리는 Needham 과 Schroeder 의 모델에 근거하여, 신뢰 받는 제 3 자인 중앙 인증 서버가 네트워크 상의 모든 개체와 서로 다른 비밀 키를 공유하고 그 비밀 키를 알고 있는 것으로 실체를 증명한다. 이에 클라이언트는 중앙 인증 서버에 자신의 신원을 증명 해 줄 것을 요청하고 중앙 인증 서버는 클라이언트에게 티켓을 발급 해 줌으로써 클라이언트의 신원을 보증한다. 클라이언트는 이 티켓을 제시하여 서버에게 서비스를 요청하고 서버는 티켓을 확인 후 클라이언트를 인증, 서비스를 제공한다.

Kerberos 는 패스워드를 네트워크 상에 노출시키지 않으며 대칭키 암호화 방식을 채택하여 암호화 과정에서 생기는 오버헤드가 작다는 장점이 있다. 이에 다양한 OS 및 SW 에 채택되어 널리 사용되고 있다.

2.2. Conditional Access System (CAS) [4]

CAS 는 각 사용자에게 분배한 개인 키를 이용하여 유료 컨텐츠를 적법한 사용자에게 안전하게 전송하기 위한 핵심 기술로서, 기존 디지털 TV 및 위성 방송, IPTV 등에서 컨텐츠 보호를 위해 사용되고 있다.

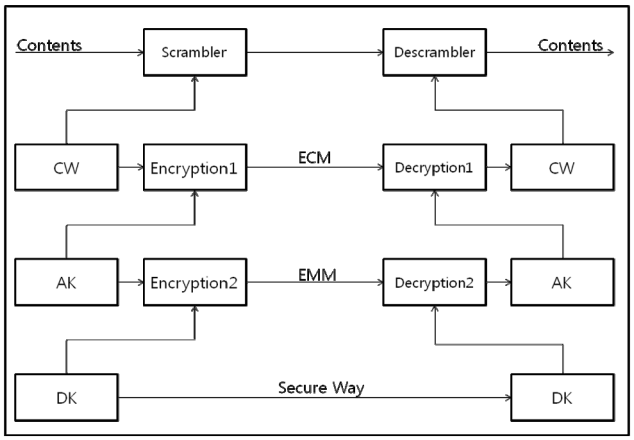

그림 1. CAS 의 구조

그림 1 과 같이, CAS 는 여러 단계의 키 관리 구조를 가지고 있는데, 이는 스트리밍 서비스에서 잦은 암호화로 인해 발생하는 부담을 분산시킴과 동시에 모든 사용자에게 동일하게 암호화 된 컨텐츠를 전송함으로써 사용자 개개인에게 다른 키를 이용하여 암호화 하는 것에 비해 컨텐츠 전송자가 갖는 암호화의 부담을 줄일 수 있게 한다.

CAS 의 구체적인 동작 과정은 다음과 같다. 우선 서버에서 전송하는 컨텐츠는 CW 에 의해 암호화 되어 ECM(Entitled Control Message)과 함께 전송되는데, 이 때 ECM 에는 해당 방송의 수신 조건 및 CW 의 정보를 담고 있으며 이 정보는 AK 에 의해 암호화 되어 있다. 이 후 AK 는 각 사용자에게 주어진 DK 로 암호화되어 EMM(Entitle Management Message)에 담겨 사용자에게 전송된다. 따라서 사용자가 암호화 된 컨텐츠를 복호화 하기 위해서는 서비스 제공자로부터 분배 받은 DK 를 이용하여 EMM 과 ECM 을 복호화 해야 한다. 이 복호화를 통해 사용자는 CW 를 얻어 암호화 된 컨텐츠를 복호화하여 시청할 수 있다.

위와 같은 CAS 의 키 관리 구조는 댁내 STB(Set-Top Box)에 삽입되는 스마트카드에 DK 를 담아 물리적으로 분배하는 것을 기반으로 하여 그 안전성을 보장한다. 이는 적합한 사용자만이 해당 키를 가지고 있다는 것을 전제로 하여 키 분배뿐 아니라 사용자 인증의 역할도 동시에 수행한다.

그러나 Open IPTV 환경에서는 STB 와 같은 특정 단말에 귀속된 서비스가 아닌 다양한 기기를 대상으로 하여 서비스를 하는 것을 목표로 하고 있기 때문에 STB 에 삽입하는 스마트 카드를 이용한 물리적인 키 분배는 적합하지 않다. 또한 Open IPTV 환경에서의 컨텐츠 제공은 특정 IPTV 사업자 하나에 의한 것이 아니라 다수의 일반인이 컨텐츠 제공자가 될 수 있기 때문에 다대다(many-to-many) 환경에서의 사용자 인증 및 키 분배 시스템을 적용하는 것이 필요하다.

3. Kerberos 기반의 사용자 인증 및 키 분배 시스템

본 논문에서는 Open IPTV 가 갖고 있는 다대다 환경에서의 사용자 인증 및 키 분배를 위하여 분산 컴퓨팅 환경에서 사용자 인증을 제공하는 중앙 집중형 인증 방식인 Kerberos 를 기반으로 한 시스템을 제안하고 이 과정을 통해 분배 된 키를 이용하여 CAS 를 Open IPTV 에 적용 시킨다.

3.1. Notations

$C_1,C_2,\ldots,C_N$	서비스 사용자 및 컨텐츠 제공자
$ID_{C1},ID_{C2},\ldots ID_{CN}$	각 서비스 사용자 및 컨텐츠 제공자의 ID
AS	인증 서버
TGS	티켓 발급 서버
K_C	C 와 AS 간의 비밀키
$K_{C1,C2}$	C_1 과 C_2 간의 공유키
T_S	C 가 S 에게 접근하기 위한 티켓 $\{S\|\|C\|\|addr\|\|timestamp\|\|lifetime\|\|Ks,c\}K_S$
A_C	C 의 authenticator 본인 인증 목적으로 S 에게 전달 $\{C\|\|addr\|\|timestamp\}K_{S,C}$
$\{M\}K_X$	X 의 비밀키로 암호화 된 메시지
AK	Authentication Key ECM 을 암호화
CW	Control Word 컨텐츠를 암호화
ECM_{AK}	CW 를 AK 로 암호화 하여 전송되는 메시지

3.2. 가정 사항

AS 는 모든 서비스 사용자 및 컨텐츠 제공자와 비밀키를 사전에 공유하며, TGS 는 서비스 사용자의 권한 정보를 담은 데이터베이스를 가지고 있다고 가정한다. 서비스 사용자가 한 번 로그인 하여 인증 받은 후에는 해당 권한 정보는 변경되지 않으며 변경 된 권한 정보는 다음 로그인 시 반영된다.

3.3. 서비스 사용자의 최초 인증 및 키 분배

서비스 사용자 C_1 은 여러 컨텐츠 제공자에게 서비스를 요청하기 위해서 IPTV service provider 에 존재하는 신뢰할 수 있는 제 3 자인 AS 에 본인의 인증을 요청한다. 이에 AS 는 C_1 의 신원을 파악하고 TGS 에 접근할 수 있는 권한을 준다.

$C_1 \rightarrow AS: ID_{c1}, tgs$
$AS \rightarrow C_1: \{K_{c1}||tgs||T_{tgs}\}K_{c1}$

C_1 은 AS 로부터 받은 티켓을 TGS 에 제시하고 자신이 서비스를 받을 수 있는 컨텐츠 제공자에게 접근할 수 있는 권한을 요청한다. TGS 는 C_1 이 제시한 티켓을 통해 신원을 파악하고 기존에 가지고 있는 C_1 의

방송 시청 권한 정보를 바탕으로 하여 C_1 이 접근할 수 있는 모든 컨텐츠 제공자에 해당하는 티켓 및 C_1 과 컨텐츠 제공자 간의 공유키를 생성, 전달한다.

$C_1 \rightarrow TGS$: T_{tgs}, $\{A_{C1}\}K_{c1,tgs}$
$TGS \rightarrow C_1$: $\{T_{c2}||T_{c3}||\ldots||T_{cN}||K_{c1,c2}||K_{c1,c3}||\ldots||K_{c1,cN}\}K_{c1,tgs}$

C_1 은 자신이 원하는 컨텐츠 제공자인 C_2 에게 TGS 로부터 발급 받은 티켓을 전달하며 서비스를 요청하고, 컨텐츠 제공자는 티켓 확인 후 둘 간의 공유키를 이용하여 자신이 전송 중인 방송의 AK 를 암호화 하여 전송한다.

$C_1 \rightarrow C_2$: $\{A_{C1}\}K_{c1,c2}$, T_{c2}
$C_2 \rightarrow C_1$: $\{timestamp+1, AK\}K_{c1,c2}$

C_1 은 C_2 로부터 받은 AK 를 이용하여 ECM 을 복호화 하고 그렇게 얻어낸 CW 를 이용하여 C_2 가 전송하는 암호화 된 컨텐츠를 복호화 하여 시청한다.

$C_2 \rightarrow C_1$: ECM_{AK}, $\{Contents\}CW$
C_1: $Decrypt\{ECM_{AK}\}$, $Decrypt\{\{Contents\}CW\}$

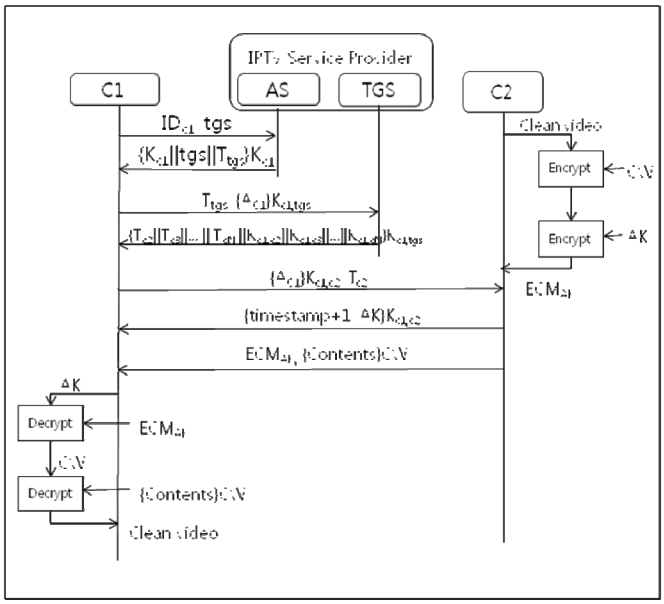

그림 2. Open IPTV 에서의 사용자 인증 및 키 분배

3.4. 채널 변경 시 사용자 인증

최초 인증 시 서비스 사용자 C_1 은 TGS 로부터 자신이 접근 가능 한 모든 컨텐츠 제공자의 티켓과 공유키를 전달받았으므로 AS 에 신원 인증을 요청하는 단계를 생략하고 가지고 있는 티켓을 이용하여 다른 컨텐츠 제공자에게 서비스를 요청할 수 있다. 이는 서비스 사용자의 인증 단계를 간소화함으로써 다른 컨텐츠 제공자로의 서비스 요청, 즉 채널 변경 시 발생할 수 있는 딜레이를 줄일 수 있다.

$C_1 \rightarrow C_N$: $\{A_{C1}\}K_{c1,cN}$, T_{cN}
$C_N \rightarrow C_1$: $\{timestamp+1, AK\}K_{c1,cN}$

4. 결론 및 향후 연구

Open IPTV 는 다양한 기기에 적용 가능한 오픈 플랫폼을 기반으로 한 서비스를 목표로 하고 있기 때문에 기술적으로 적합한 웹 기반의 플랫폼이 특히 주목받고 있다. 이러한 환경에서 이미 웹 보안 서비스로서 충분히 안전성을 검증 받아 온 Kerberos 를 Open IPTV 에 적용하는 것은 효과적이라고 볼 수 있다.

또한 기존 IPTV 에서 사용 된 스마트카드를 이용한 물리적인 키 분배 방법 대신 Kerberos 인증 메커니즘을 이용한 안전한 키 분배 방법을 사용함으로써 스마트카드를 읽을 수 없는 일반 PC, 모바일 기기 등에서도 CAS 를 적용하기 위한 키 분배를 할 수 있다. 이는 기기에 구애 받지 않고 서비스를 하고자 하는 Open IPTV 의 목적에 알맞다.

Open IPTV 는 아직 그 연구가 초기 단계에 있지만, 스마트폰의 어플리케이션, 위키피디아, 유튜브 등 오픈 된 환경에서 일반인의 참여를 통해 큰 창출 효과를 얻은 사례를 생각할 때, Open IPTV 가 갖는 가능성은 무궁무진 할 것이라 예상할 수 있다. 그러나 오픈 된 환경이란 그만큼 보안상의 허점을 가질 수 있는 만큼 효과적으로 적용될 수 있는 안전한 메커니즘의 개발이 필요하다.

이에 본 논문에서는 여러 컨텐츠 제공자가 존재 할 수 있는 Open IPTV 환경에서 Kerberos 를 기반으로 한 단말기에 독립적인 사용자 인증 및 키 분배 메커니즘을 제안하였다.

향후에는 Kerberos 를 Open IPTV 환경에 맞게 수정, 보완하여 시뮬레이션을 통해 그 성능을 증명할 예정이다.

참고문헌

[1] Mats Cedervall, Uwe Horn, Yunchao Hu, Ignacio Mas Lvars, Thomas Nasstrom, “Open IPTV Forum – Toward an Open IPTV Standard,” Ericsson Review, No.3, 2007.
[2] Open IPTV Forum, “Functional Architecture V2.0,” http://www.openiptvforum.org/
[3] Neuman, B.C, Ts’o, T., “Kerberos: an Authentication Service for Computer Networks,” IEEE Communication Magazine, Vol.32, No.9, Sep. 2004.
[4] Fu-Kuan Tu, Chi-Sung Laih, Hsu-Hung Tung, “On Key Distubution Management for Conditional Access System On Pay-TV System,” IEEE Transactions on Consumer Electronics, Vol.45, No.1, Feb. 1999.