IPTV에서 PKI/PMI기반의 권한 제어시스템

왕수* · 조인준*

*배재대학교

PKI/PMI based Access Control System on IPTV

Wang Shuai* · In-June Jo *

* Pai Chai University

요 약

현재 통신·방송 융합 서비스로 크게 대두되고 있는 서비스는 IPTV 서비스이다. IPTV 서비스는 대량의 방송 채널 선택, VoD서비스, 각종 양방향 응용 서비스 등과 같은 고품질의 다양한 방송·통신 융합 서비스 제공한다. IPTV에 대한 관련 기술이 빠르게 발전되면서 그에 대한 불법시청, 불법 복제, 접근권한 오남용 등 IPTV 콘텐츠 보안취약점에 대한 우려가 증가되고 있는 추세이다. 본 논문에서는 공개키 기반구조(PKI)의 공개키 인증서와 권한인증기반구조(PMI)의 속성인증서를 이용하여, 콘텐츠 서버 접근통제방안을 제안하였다.

ABSTRACT

IPTV, which is convergence of Communication and Broadcasting, has improved quickly recently. This service can provide high quality and various services to their customers, such as choosing channels freely, VOD and many kinds of Interactive service. As the technology of IPTV rapid development, more and more people worry about its disadvantages during the spread and apply, for instance, the illegal application, illegal copy, access authority abuse and the danger of the IPTV contents. This paper will provide the solution to solve these problems, through the Public Key Certificate of PKI(Public Key Infrastructure) and the Attribute Certificate of PMI(Privilege Management Infrastructure).

키워드

IPTV, PKI, PMI, 접근제어

Ⅰ. 서 론

IPTV 서비스는 통신 기술이 발달함에 따라 불법 콘텐츠 제공자, 불법 콘텐츠 시청자, 부당한 시청권한 부여 등 취약점을 가지고 있다. 이를 해결하기 위해 본 논문에서는 IPTV환경에서 신원인증시 PKI인증서(PKC)로 신원인증을 하고 보안과 접근 제어는 PMI에서 제어하는 PMI인증서(AC)를 이용하는 권한인증시스템을 구현하였다. 따라서 사용자가 로그인하면 기존의 신원 인증서(PKC)와 그에 해당하는 속성 인증서(AC)에 정의되어있는 권한에 의한 접근제어를 하며 권한관리 모델에서 관리 적인 측면에서 보다 손쉽고 효과적인 접근제어정책을 관리할 수 있는 룰 기반의 PKI/PMI시스템을 제안하고자 한다[1][2][3].

Ⅱ. 본 론

이 장에서는 제안한 PKI/PMI를 이용한 접근제어 시스템에 대하여 상세히 기술한다. 본 시스템은 IPTV 단말기, Access Controller, 콘텐츠 서버, PKI/PMI 아키텍처, 콘텐츠 서버 등으로 나뉘어진다. <그림 2.1>은 본 시스템의 전체적인 구성도이다.

PKI/PMI 모델의 방법은 사용자가 원하는 방송을 시청하기위하여 콘텐츠 서버에게 자원요청을 한다. 사용자가 공인된 인증기관에서 공개키 인증서를 획득한 다음 전자 서명을 하고 Access Controller를 통하여 콘텐츠 서버에게 전송하고 콘텐츠 서버는 자기 인증서를 전자 서명하고 Access Controller를 통하여 사용자에게 전송한다. PEP가 공인된 인증기관을 통하여 전자 서명된 공

개키 인증서가 유효한지를 검사한다[4][5].

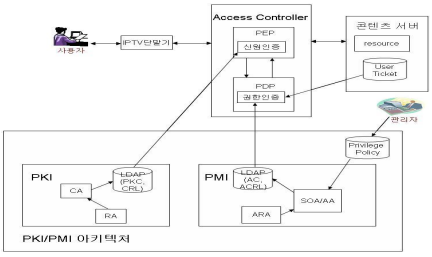

그림 2.1 전체 시스템 구성도

이와 같이 사용자와 콘텐츠 서버가 서로 신원 확인을 거치고, 콘텐츠 서버가 상호 인증하는 사용자 티켓을 사용자에게 부여하며, PDP가 인증된 신원에 의하여 PMI LDAP에 저장된 속성 인증서를 검색하고, 속성 인증서를 분석하여 사용자 사용 정책을 획득한다. 획득한 정책을 사용자 요구와 비교하고 권한이 있으면 콘텐츠 서버는 Sessionkey로 암호화된 방송을 시청할 수 있다. 본 논문에서는 이 시스템을 이용하여ID와 Password를 부여하고 인증하는 방식을 사용하지 않고 사용자가 Usbkey를 STB에 꽂아서 PIN을 입력하여 인증을 거치고 Usbkey에 저장된 공개키 인증서, 개인키, 사용자 티켓 등을 통하여 안전한 인증방식을 제공하여 속성 인증서에 정의된 권한에 의하여 콘텐츠 서버를 접근하게 되는 시스템을 구현한다.

2.1 공개키 생성 단계

사용자, 사용자들에 대한 속성 인증서를 발급하고 관리하는 기관인 속성인증기관, 사용자 접근 요청을 분석하고 허가 또는 거부를 결정하는 Access Controller, 콘텐츠를 제공하는 콘텐츠 서버, 이들이 공개키 기반구조상의 인증기관으로부터 인증서를 신청하는 방법이 같기 때문에 여기서 사용자가 인증서발급과정만을 분석한다. PkI 인증서 신청 과정은 다음 <그림 2.2>와 같다.

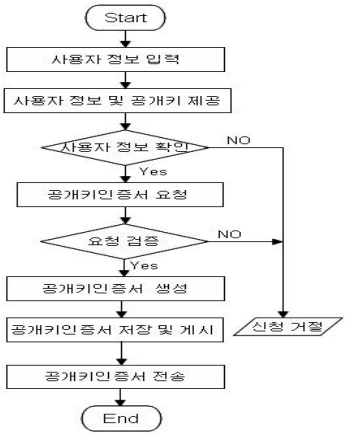

그림 2.2 PKI 인증서 신청 과정

① 사용자는 공개키 인증서를 신청하기 위하여 RA에 접속하여 자신의 식별자IDc, 사용자 정보와 공개키KUc 등을 전송한다.

② 사용자 정보를 수신 받은 RA는 사용자 신원 유효성을 검증하고 CA에 사용자 인증서를 요청한다. 사용자의 식별자IDc, 사용자 정보와 공개키KUc를 CA에 함께 정송한다.

③ CA는 수신하는 정보에 의하여 사용자 공개키 인증서 내용을 추가하고 자기 개인키를 사용하여 사용자 공개키를 서명하여 사용자 공개키 인증서를 생성하고 이에 대한 정보를 디렉토리 서버 LDAP를 통하여 엔트리에 게시한다. 사용자 공개키 인증서와 인증기관 공개키를 사용자에게 전송한다.

2.2 정책 정의 단계

서버 관리자는 웹 서버를 통하여 콘텐츠 정보를 저장되어 있는 콘텐츠 서버에 접근할 수 있도록 Role를 생성하고 Role별 접근제어 정책을 설정한다. 정책 정의 과정은 다음 <그림 2.3>과 같다.

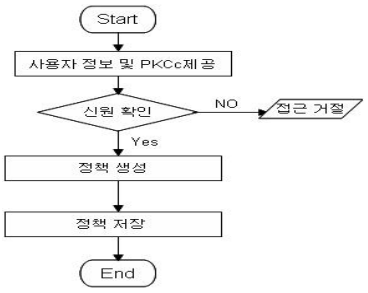

그림 2.3 정책 정의 과정

① 서버 관리자는 Privilege Policy에게 접근하기 위하여 자신의식별자 IDs와 공개키 인증서 PKCs를 서명하여 전송한다.

② IDs와 공개키 인증서PKCs를 검증하고 인증하는 경우에 서버 관리자는 Role를 생성하고 Role별 접근제어 정책을 설정한다.

2.3 PMI 인증서 생성 단계

① 사용자<그림2.4>는 접근하고자 하는 콘텐츠 서버의 서비스를 요청하기 위하여 ARA에 접속하여 자신의 공개키 인증서와 속성 인증서 요청 패킷에 서명하여 이를 ARA에 전송한다.

② ARA는 사용자의 공개키를 이용하여 사용자의 신원을 확인하고, 사용자로부터 속성 인증서 요청 패킷의 서명문을 확인하고 서명문을 추출하여 ACA에 전송한다. 사용자의 요청 패킷에는 사용자가 접속하고자 하는 서버와 응용서비스에 대한 요구내용이 포함된다.

③ Privilege Policy DB에서는 시스템관리자가 설정한 보안정책을 검토하여, 사용자의 요구가 적합한지를 확인하고 적법한 경우에는 속성 인증서

를 발급하고 이를 디렉토리 서버에 저장하고 게시한다.

④ 속성 인증서 신청결과를 사용자에 전송한다.

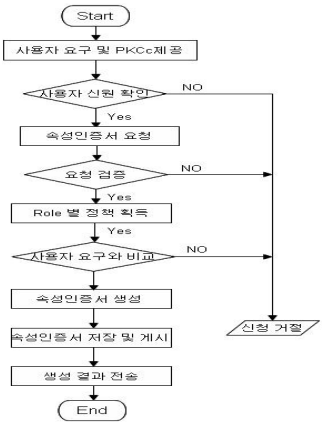

그림 2.4 PMI 인증서 신청 과정

2.4 상호 인증 단계

사용자는 콘텐츠 서버 서비스를 사용하기 위하여 서로 신원인증을 하고 콘텐츠 서버로부터 정송 받은 사용자 티켓을 가지고 서비스 사용권한을 있는 사용자만 서비스를 사용할 수 있다. 사용자와 콘텐츠 서버 상호 인증 과정은 <그림 2.5>와 같다.

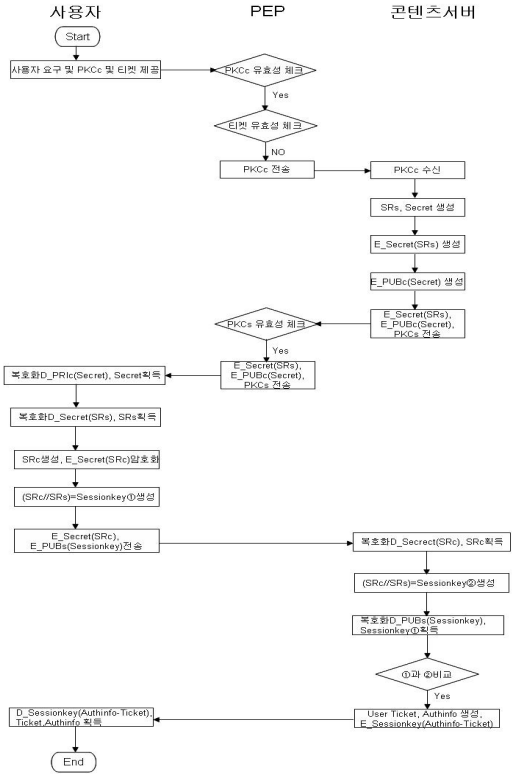

그림 2.5 사용자와 콘텐츠 서버 상호 인증 과정

① 사용자는 콘텐츠 서버를 접속하기 위하여 자신 Usbkey안에 저장되어 있는 공개키 인증서, 콘텐츠 서버에 접속하여 사용하고자 하는 서비스에 대한 서비스요구패킷, 사용자와 콘텐츠 서버 상호 인증하여 받은 사용자 티켓(상호 인증 전에 사용자 티켓 없음)을 Access Controller에 전송한다[6][7][8].

② 수신 받은 Access Controller의 PEP를 사용하고 공개키 인증서의 유효성을 확인하기 위하여 PKI LDAP에서 검색하여 비교하고, 적법한 경우에는 사용자의 티켓유효성을 확인하기 위하여 User Ticket DB에서 검색하여 비교한다.

③ 사용자가 티켓이 없거나 사용자 티켓이 무효인 경우에 PEP는 사용자의 공개키가 콘텐츠 서버에 전송된다. 콘텐츠 서버는 SecureRandom함수를 이용하여 난수(SRs)를 생성하고, 이를 SEED 기반의 비밀키(Secretkey)를 사용하여 암호화 한다(E_SRs_Secretkey). Secretkey를 안전하게 전송하기 위하여 사용자의 공개키(PUBc)를 사용하여 암호화한다(E_Secretkey_PUBc). 콘텐츠 서버는 Access Controller의PEP를 통하여 자신의 인증서(PKCs), E_SRs_Secretkey, E_Secretkey_PUBc를 사용자에게 전송한다.

④ PEP는 콘텐츠 서버 인증서 유효성을 확인하기 위하여 PKI LDAP에서 검사한다. 인증서가 유효한 경우에, PEP가 전송 받은 정보를 사용자에게 전송한다. 사용자는 자신의 개인키(PRIc)를 사용하여 콘텐츠 서버로부터 수신한 Secretkey를 복호화 한다(D_Secretkey_PRIc). 복호화한 Secretkey를 사용하여 SRs를 복호화 한다(D_SRs_Secretkey). 사용자는 자신의 난수(SRc)를 생성하고, 이를 Secretkey로 암호화한다(E_SRc_Secretkey). 사용자는 자신이 생성한 SRc와 복호화한 SRs를 연접(SRc//SRs)하여 32바이트의 세션키를 생성하고 이를 콘텐츠 서버 공개키(PUBs)를 사용하여 암호화한다(E_Sessionkey_PUBs). 사용자는 E_SRc_Secretkey와 E_Sessionkey_PUBs를 콘텐츠 서버에게 전송한다.

⑤ 콘텐츠 서버는 Secretkey를 사용하여 SRc를 복호화 한다(D_SRc_Secretkey). 복호화한 SRc와 콘텐츠 서버 자신의 SRs를 연접하여, 32바이트 세션키를 생성한다(SRc//SRs). 콘텐츠 서버의 개인키를 사용하여 사용자부터 수신한 세션키를 복호화 하고 콘텐츠 서버 생성한 세션키를 비교한다. 두 키가 일치한다면 세션키를 동기화하고 사용자티켓을 생성하고, 인정이 성공했음을 알리는 메시지를 함께 동기화한 세션키를 사용하여 암호화한다(E_Authinfo-Ticket_sessionkey).

⑥ 사용자는 세션키로 Authinfo-Ticket를 복호화(D_Authinfo-Ticket_Sessionkey)하여 인증이 성공했음을 알게 되고 사용자티켓을 Usbkey에 저장한다.

2.5 접근 인증 단계

① 사용자<그림2.6>는 콘텐츠 서버를 접속하기 위하여 자신 Usbkey안에 저장 있는 공개키 인증서와 콘텐츠 서버에 접속하여 사용하고자 하는 서비스에 대한서비스요구패킷, 사용자와 콘텐츠 서버 상호 인증하여 받은 사용자 티켓을 Access Controller에 전송한다.

② 공개키 인증서 유효성을 확인하기 위하여 수신 받은 Access Controller의PEP를 사용해서 PKI LDAP에서 검사한다. 유효한 경우에는 사용자 티켓유효성을 확인하기 위하여 콘텐츠 서버에서 저장된 사용자티켓을 검색하여 비교한다. 요청하는 메시지를 분석하고 정확한지를 확인한다. 이들을 다 확인한 후에 사용자신원과 요청 패킷을 PDP에 전송한다.

③ PDP는 사용자 신원에 의하여 사용자 속성 인증서를 저장된 PMI LDAP중에 이 신원과 대응한 속성 인증서를 검색하여 속성 인증서 대응한 역할 메시지를 PEP에 반환한다. 반환된 역할을 근거하여 Privilege Policy DB중에 이 역할과 대응하는 권한을 검색하여 사용자 요청과 비교하여 허가/거부 여부를 다시 PEP에 전송한다.

④ 허가하는 경우에 PEP는 요구패킷을 콘텐츠 서버로 전송한다. 콘텐츠 서버는 동기화한 세션기를 사용하여 사용자 원하는 내용을 암호화하여 사용자에 전송한다. 거부하는 경우에 거절 패킷을 사용자로 전송한다.

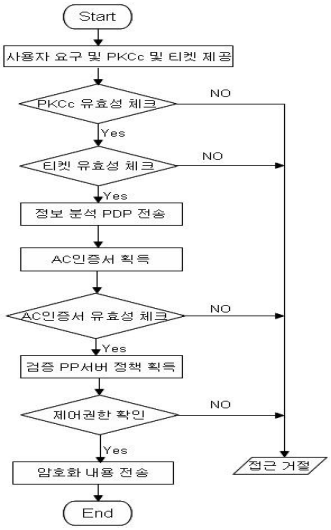

그림 2.6 서비스 시청 과정

Ⅲ. 결 론

IPTV는 많은 장점을 가지고 있지만 관련 기술과 표준 확립, 관련 법규의 불 완비는 서비스 활성화의 걸림돌이 되고 있다. 무엇보다도 사용자의 인증정보 및 속성 등의 보안에 관련한 문제가 있다. 양방향 서비스를 이용한 T-Commerce와 댁내 가전의 제어를 위한 보안의 중용성이 서비스의 제공자나 사용자에게 민감할 수밖에 없기 때문이다.

위와 같은 문제점을 해결하기 위해 본 논문에서는 PKI/PMI 권한제어 시스템을 설계하고 구축하였다. 즉 PKI기술과 PMI기술을 용합한 권한제어 시스템 이다. 사용자와 콘텐츠 제공자는 상호 인증하여 사용자에게 티켓을 전송하고 Session키를 성생한다. 이 Session키로 콘텐츠를 암호화하여 사용자에게 전송한다. 사용자가 자원에 접근할 때 적용된 속성인증에 따른 Role에 정의된 권한에 의해 사용자 허가/거부를 하는 방법으로써 기존의 ECM, EMM 사용하여 전송하는 방식이 필요 없다.

참고문헌

[1] 최락권,양준환,"IPTV서비스 현황과 진화 방향",한국 인터넷 정보학회 제8권 제11호 3, 2007

[2] 류원옥,조기성,이병선,"IPTV 서비스 제어 구조 동향",주간기술동향 통권 1340호 4, 2008

[3] ITU-T FG WG3,Working Document: IPTV Security Ascepts,FG IPTV-DOC -0122, Geneva: ITU-TFGIPTV, 7. 22, 2007

[4] Ryutov T., Neuman C., Pearlman L Generic Authorization and Access Control Application Program Interface C-bindings <draft-ietf-cat-gaa-cbind-05.txt> [EB/OL].http://www.isi.edu/gost/info/gaaapi/, 11.2000

[5] Xu Xiuling, Li Daxing,"The Research and Design of SSO System" Shandong University Master's Thesis, 4, 2008

[6] Tian Xiaofei, Shi Yan,"Study on Workflow Access Control Model Based on PKI/PMI" Southwest Jiaotong University Master's Thesis, 7, 2008

[7] Sandhu R, Coyne EJ, Feinstein HL, Youman CE. Role-Based access control models, IEEE Computer, 1996, 29(2)

[8] Sharon Boeyen. X.509 4th edition: Overview of PKI&PMI Frameworks (Entrust Inc.)<http://www.entrust.com/resources/pdf/509_overview.pdf> 2000