IPTV에서 PKI기반의 안전한 인증시스템

왕수* · 조인준**

Based PKI System for Secure Authentication on IPTV

Wang Shuai* · In-June Jo**

요 약

IPTV는 방송과 통신의 대표적인 융합서비스이다. 이는 가입자들의 요구를 만족시키는 다양한 콘텐츠와 더불어 효율적인 서비스를 제공한다. IPTV 가입자들이 급격하게 증가함에 따라서 콘텐츠 제공자들이 늘어나고 있다. 따라서 불법 콘텐츠 시청자, 부당한 시청권한 부여 및 서비스 제한을 방지하기 위해 안전한 인증시스템을 필요로 한다. 이에 본 논문에서는 PKI기반을 이용하여 키 정보를 생성하고 IPTV 가입자들에게 생성한 키를 안전하게 분배하고 IPTV 가입자와 콘텐츠 제공자의 신분 인증 기능을 수행하는 방안을 제안하였다. 제안시스템은 안전성 있고 효율적인 상호 신분 확인 및 인증을 제공한다.

ABSTRACT

IPTV service is one of the representatives for the integration of broadcasting industry and communication industry, which also can meet users' various demands and provide efficient service. As the increasing number of IPTV users and contents servers, it is necessary to provide the safety authority system to prevent the illegal audio-visual, incorrect audio-visual authority, and illegal authority control. This thesis puts forward PKI(Public Key Infrastructure) as the foundation key production mechanism. Through this mechanism, the key can be transferred safely to users and authenticate the ID of users and contents servers. In a word, our system can provide safe and efficient service for mutual authentication

키워드

IPTV, PKI, illegal audio-visual, mutual authentication

* 배재대학교 컴퓨터공학과 석사과정

** 배재대학교 컴퓨터공학과 교수(교신저자)

접수일자 2008. 12. 15

심사완료일자 2009. 03. 17

Ⅰ. 서 론

IPTV의 새로운 서비스는 기존 방송서비스와 통신서비스가 결합된 형태다. 특징으로는 주로 양방향성과 실시간 서비스 제공을 들 수 있다. 최근에는 ITU-T를 중심으로 IPTV에 대한 국제표준화가 시작되고 있다. IPTV가 위성/케이블/지상파 방송과 함께 중요한 방송 매체로 자리 잡고 더 나아가 통신과 방송이 융합되는 현 시점에서 그 중심이 될 것으로 전망되고 있다.

ITU-T FG IPTV에서는 IPTV를 "서비스에서 요구하는 QoS/QoE를 제공하고, 보안과 양방향성 및 신뢰도를 보장할 수 있도록 관리 할 수 있는 IP 기반의 네트워크를 통해 텔레비전/비디오/오디오/텍스트/그래픽/데이터 등을 전달하는 멀티미디어 서비스"라고 정의하고 있다[1].

IPTV 가입자들이 증가함에 따라 불법 콘텐츠 시청자, 부당한 시청권한 부여 및 서비스 제한은 늘어나고 있다. 이를 방지하기 위한 연구노력이 계속되고 있으며 좀 더 안전하고 효과적인 가입자의 신분과 콘텐츠 제공자의 신분 인증 방법이 필요하다. 기존 방송 서비스에서 사용하는 CAS(Conditional Access System)는 단방향 방송 구조를 바탕으로 도입되었기 때문에 Request/Response 방식을 사용할 수 없다. 그리고 필요하지 않은 ECM (Entitlement Control Message)때문에 트랜스포트 스트림의 대역폭을 낭비한다. 수신자격 정보를 가진 EMM (Entitlement Management Massage)또한 방송 매체를 통해 전송된다. 한 매체의 대역폭을 모든 이용자가 공유하는 방송의 특성상 특정 목적 STB를 향하는 모든 EMM은 대역폭을 항상 낭비하게 된다. 그리고 기존의 STB(Set Top Box)는 대부분 스마트카드를 이용하고 스마트카드 내의 복호화 알고리즘이나 비밀키를 주기적으로 갱신해주어야 한다. 또한 대부분 디스크램블러와 스마트카드가 일체화 되어 있는 형태이다. 이들은 자신의 IPTV STB가 설치되어 있지 않은 다른 장소에서는 시청을 할 수 없다.

이러 문제를 해결하기 위해서 본 논문에서는 스마트카드를 발급받을 필요 없이 가입자가 자신의 ID와 패스워드만을 가지고 디스크램블러가 설치된 어떠한 장소에서도 IPTV방송 시청이 가능한 새로운 PKI(Public Key Infrastructure)기반의 안전한 인증시스템을 제안하였다. 제안한 시스템은 인증서를 사용하여 세션키와 공개키의 조합으로 효율적인 인증 및 전자서명 기능을 제공한다. 인증서는 개인 또는 기관에서 서명 및 암. 복호화에 사용되는 공개키와 이에 대응한 개인키의 소유 증명을 확인해 주는 전자매체로써 각 가입자의 신원을 증명하기 위해 중요한 수단이다.[2]

본 논문의 구성은 다음과 같다. 1장의 서론에 이어. 2장에서는 IPTV 가입자를 위한 PKI 시스템을 설계하고 동작 시나리오를 설명하였다. 3장에서는 CA 시스템을 설계하고 기능 수행 절차를 분석하였다. 마지막으로 4장에서는 결론을 도출하였다.

Ⅱ. 본 론

2. PKI 시스템

2.1 PKI 시스템 구성 및 기능

본 논문에서의 PKI시스템은 사용자 인증을 공개키 알고리즘을 이용해서 전자적으로 구현한 인증 시스템을 제안하고 있다. 본 시스템을 사용하는 사용자는 인증, 무결성, 부인방지, 접근통제 등 인터넷 환경에서 요구되는 다양한 보안 서비스를 제공받게 된다.[3][4]

본 논문에서 연구한 IPTV 가입자를 위한 PKI 시스템은 그림 1과 같은 시스템 구성을 가지고 있다.

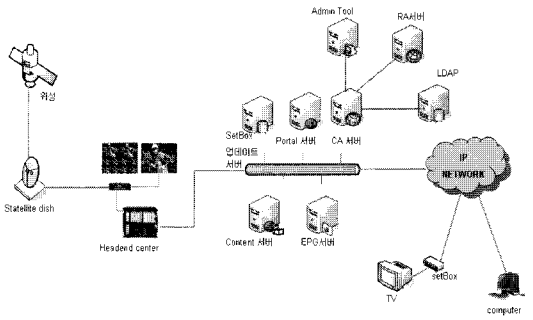

그림 1. IPTV를 위한 PKI 인증시스템 구조도
Fig 1. Based PKI system structure for secure authentication on IPTV

CA 서버: 인증서를 발급하고 관리하는 인증 시스템의 핵심으로 다양한 공개키 알고리즘을 통하여 사용자 인증서를 발급한다.

RA 서버: 사용자 정보를 등록하고 관리하는 시스템으로 CA 서버와 연계하여 사용자 인증서에 대한 발급 업무를 보조해준다.

LDAP(Lightweight Directory Access Protocol): CA 서버에서 발급한 인증서를 공표하기 위한 시스템으로 공개저장소의 개념을 포함한다.

Admin Tool: CA 서버에 대한 운영 및 관리를 위한 관리자 전용 도구로 CA 서버에 대한 전반적인 운영을 제어할 수 있다.

Portal 서버: EPG 서버와 연계하여 가입자의 패스워드를 관리하고 가입자 신분인증을 제공한다.

콘텐츠 서버: IPTV 가입자들에게 VOD서비스, EPG 서비스, VoIP, SMS, 메시징 서비스, TV쇼핑, 홈뱅킹, 웹 검색 서비스를 제공하는 서버이다.

STB 업데이트 서버: STB 버전을 관리하고 STB 업데이트 사용하는 시스템이다.

EPG(Electronic Program Guide)서버: 채널, VOD,양방향 데이터 서비스에 대한 메뉴 및 상세 정보를 제공하고 관리하는 시스템의 핵심으로 다양한 정보를 사용자에게 전송한다.

2.2 동작 시나리오

(1) 가입자가 프로그램 시청을 원할 경우 리모컨을 사용하여 자신의 ID와 패스워드를 입력하게 되고, 이를 입력받은 가입자 STB를 통하여 Portal 서버에 전송한다.

(2) Portal 서버는 EPG 서버와 연결하고 입력된 가입자의 패스워드, ID 및 EPG버전이 검증된 후 가입자가 정당한 소유자 인지 검증한다.

(3) EPG 서버는 입력된 가입자의 EPG 버전에 비교하여 STB 업데이트의 필요성여부를 판단한다. 업데이트가 필요한 경우에, STB 업데이트 서버를 통해 업데이트를 한다.

(4) 상기2)의 결과가 정당한 소유자로 검증된 경우에, STB는 가입자 인증 메시지를 생성하여 IP망을 통하여 CA 서버에게 전송한다.

(5) CA 서버는 수신한 가입자 인증메시지를 이용하여 가입자가 정당한 IPTV 가입자인지 검증한다. 검증이 성공하면 콘텐츠 서버에게 성공메시지를 전송한다. 만약 검증이 실패한 경우에는 동작이 종료된다.

(6) 상기5)의 과정이 성공할 경우, 콘텐츠 서버는 콘텐츠 서버 인증 메시지를 생성하여 CA 서버에게 전송한다.

(7) CA 서버는 수신한 콘텐츠 서버 인증 메시지를 수신하여 콘텐츠 서버를 검증한다. 검증이 성공하면 IPTV 가입자에게 성공 메시지를 전송한다. STB와 콘텐츠 서버간의 상호 신분 확인/인증이 완료되면 가입자는 서비스를 사용할 수 있다. 만약 검증이 실패인 경우에는 동작이 종료된다.

(8) 이상의 과정과는 별도로 가입자가 자신의 패스워드를 변경하고자 할 때에는 이전에 사용했던 패스워드를 입력하여 정당한 소유자인지 먼저 검증을 받는다.

(9) 입력된 가입자의 패스워드는 IP망을 통하여 Portal 서버에게 전송하고 검증한다. 만약 정당한 소유자가 아니면 동작이 종료된다.

(10) 정당한 소유자로 검증된 경우에, 가입자는 새로운 패스워드를 STB에 입력하고 STB는 패스워드 변경 요구 메시지를 생성하여 IP망을 통하여 Portal 서버에게 전송한다.

(11) Portal 서버는 수신한 패스워드 변경 요구 메시지를 이용하여 가입자가 정당한 가입자인지 검증한다. 만약 검증이 실패한 경우에 가입자는 Portal 서버에 저장된 가입자의 패스워드를 변경할 수 없게 된다. 검증이 성공한 경우에는 해당된 가입자의 패스워드가 변경되어 안전하게 저장된다.

(12) Portal 서버는 STB에게 변경 성공 메시지를 안전하게 전송한다. 이때는 패스워드를 변경 성공된다.

(13) STB를 이동 시켜하는 경우에 사용자가 리모컨을 사용하여 자신의 ID와 패스워드를 입력하게 되고 다시 1)을 시도 한다. STB는 재설치 할 필요가 없다.

3. CA 시스템의 기능

3.1 구성

본 논문에서 연구한 PKI 시스템에서 CA 서버가 가지는 역할은 절대적이라고 할 수 있다. CA 서버는 PKI 시스템의 근본을 이루는 사용자 인증서를 발행하기 위한 서버이다, 이를 위해서 다양한 요소를 가지게 된다. CA 서버의 역할 및 기능은 그림 2와 같다.

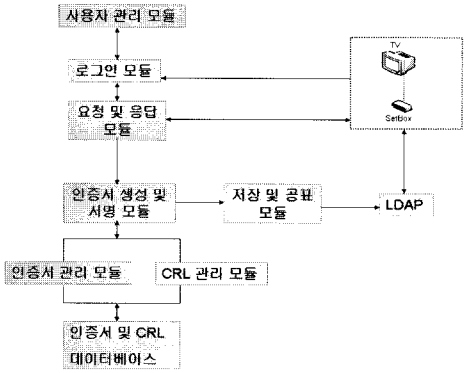

그림 2. CA 시스템의 모듈 구조도
Fig 2. Structure of CA system module

3.2 기능 수행 절차

참고문헌 [5][6][7][8]을 참고하여 본 논문에서 새롭게 제안하는 인증시스템에서는 CA에서 발급받은 인증서를 STB에 저장하고, 이를 세션키와 조합하여 안전한 인증기능을 제공한다. 인증서에서 사용하는 공개키 암호 알고리즘은 RSA를 사용하고 세션키는 SEED 암호 알고리즘을 사용하여 생성한다. 표 1은 본 논문에서 제안한 인증과정을 설계하는데 사용한 표기들이다.

표 1 사용자 인증 프로토콜 표기
Table 1. Sign of user authentication protocol

표기	의미
E	암호화(Encryption)
D	복호화(Decryption)
CA	인증기관(Certificate Authority)
STB	Set Top Box, IPTV사용자
CS	콘텐츠 서버, 인증 서버 및 서비스 제공자
CERTSTB	STB 인증서
CERTCS	콘텐츠 서버 인증서
SRSTB	STB가 생성한 난수 (Secure Random 값)
SRCS	CS가 생성한 난수 (Secure Random 값)
PRISTB, PUBSTB	STB의 개인키와 공개키
PRICS, PUBCS	CS의 개인키와 공개키
Secretkey	비밀키(Secret Key)
Sessionkey	세션키(Session Key)
AuthInfo	인증이 성공했음을 포함하는 인증 메시지
SEED	대칭 암호 알고리즘 (SEED)
RSA	비대칭 암호 알고리즘 (RSA)
SHA-1	해시 알고리즘(Secure Hash Algorithm)
‖	연접(Concatenate)연산자

3.2.1 Connection Request와 Challenge

다음 그림 3은 Connection Request와 Challenge의 동작 과정을 보여주고 있다.

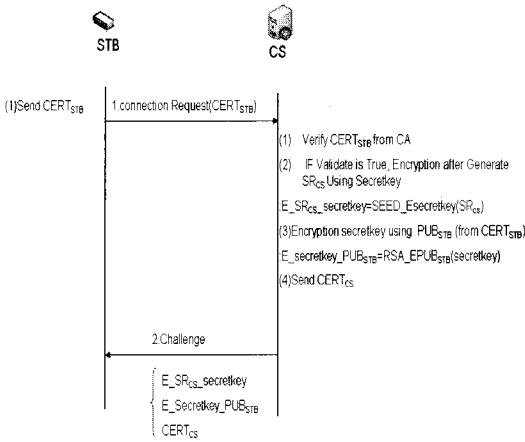

그림 3. 단계1.연결요청 와 단계2. 도전
Fig 3. Step 1.Connection request and Step 2 challenge

Step 1. [STB->CS]: STB가 콘텐츠 서버로 접속을 요청한다. 이때 STB는 자신의 인증서(CERTSTB)를 콘텐츠 서버로 전송한다.

Step 2. [STB<-CS]: 콘텐츠 서버가 E_SRcs_Secretkey와 E_Secret_PUBSTB, CERTCS를 STB로 전송한다.

① STB의 연결요청과 인증서를 수신한 콘텐츠 서버는 CA에게 인증서의 유효성 유무를 요청한다.
② STB의 인증서가 유효한 경우, 콘텐츠 서버는 SecureRandom 함수를 이용하여 난수(SRCS)를 생성하고, 이를 SEED 기반의 비밀키(Secretkey)를 사용하여 암호화 한다.(E_SRCS_Secretkey).
③ Secretkey를 안전하게 전송하기 위해, CERTSTB로부터 획득한 RSA 기반의 공개키(PUBSTB)를 사용하여 암호화 한다.(E_Secretkey_PUBSTB).
④ 콘텐츠 서버는 자신의 인증서(CERTCS)를 STB로 함께 전송한다.

3.2.2 Response

그림 4는 Response의 동작 과정을 보여주고 있다.

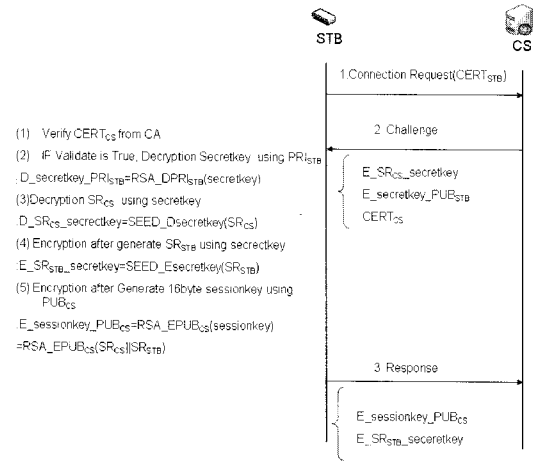

그림 4. 단계 3 응답
Fig 4. Step 3. response

Step 3. [STB->CS]: STB가 E_Sessionkey _PUBCS와 E_SRSTB_Secretkey를 콘텐츠 서버로 전송한다.

① 콘텐츠 서버로부터 인증서를 수신한 STB는 CA에게 인증서의 유효성 유무를 요청한다.

② 콘텐츠 서버의 인증서가 유효한 경우, STB는 자신의 개인키(PRISTB)를 사용하여 콘텐츠 서버로부터 수신한 Secretkey를 복호화 한다(D_Secretkey_PRISTB).

③ 복호화한 Secretkey를 사용하여 SRCS를 복호화 한다(D_SRCS_Secretkey).

④ STB는 자신의 난수(SRSTB)를 생성하고, 이를 Secretkey로 암호화한다(E_SRSTB_Secretkey).

⑤ STB는 자신이 생성한 SRSTB와 복호화한 SRCS를 연접(SRCS//SRSTB)하여 16바이트(SEED는 128비트의 키를 사용)의 세션키를 생성하고 이를 CERTCS로부터 획득한 공개키(PUBCS)를 사용하여 암호화 한다(E_Sessionkey_PUBCS).

3.2.3 Authentication Info

Step 4. [STB<-CS]: 콘텐츠 서버가 인증 유무를 알려주는 E_AuthInfo_Sessionkey 또는 Fail 메시지를 STB로 전송한다.

① Secretkey를 사용하여 SRSTB를 복호화 한다 (D_SRSTB_Secretkey).

② 복호화한 SRSTB와 콘텐츠 서버 자신의 SRCS를 연접하여, 16바이트 세션키를 생성한다 (SRCS//SRSTB).

③ 콘텐츠 서버의 개인키(PRICS)를 사용하여 STB로부터 수신한 세션키를 복호화 한다 (D_Sessionkey_PRICS).

④ 콘텐츠 서버는 ②에서 생성한 세션키와 ③에서 복호화한 세션키를 비교한다. 만약, 두 키가 일치한다면 세션키를 동기화하고 STB에게 인증이 성공했음을 알리는 메시지를 동기화한 세션키를 사용하여 암호화한다(E_AuthInfo_Sessionkey). 그러나 두 키가 일치하지 않는다면, 인증이 실패했음을 알리는 메시지를 생성한다(Fail).

그림 5는 Step 4의 과정을 보여주고 있다.

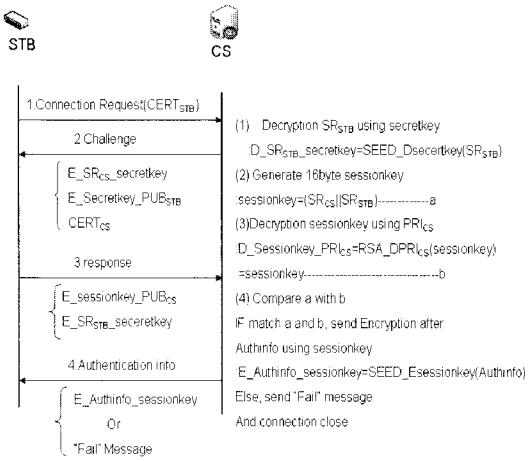

그림 5. 인증 정보
Fig 5. Step 4. authentication Info

3.2.4 Support of Application Service

Step 5. [STB<->CS]: 인증이 성공한 경우 콘텐츠 서버에게 IPTV 서비스를 제공받을 수 있다.

① 콘텐츠 서버로부터 "Fail"메시지를 수신한 경우, Step 1부터 재시도 한다.

② 세션키로 AuthInfo를 복호화 하여 인증이 성공했음을 알게 된다(D_AuthInfo_Sessionkey).

③ 동기화한 세션키를 사용하여 안전하게 메시지를 주고받을 수 있으며, 또한 콘텐츠 서버의 IPTV 서비스를 제공받을 수 있다.

그림 6은 Step 5의 과정을 보여주고 있다.

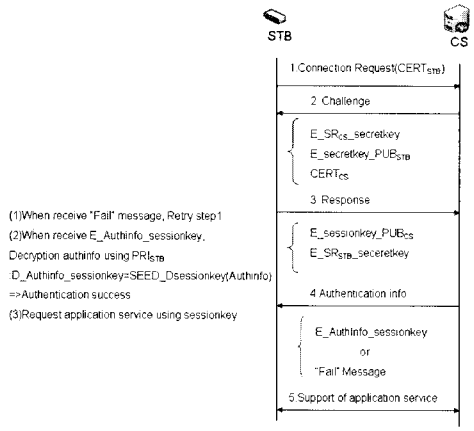

그림 6. 단계 5 응용 서비스 지원
Fig 6. Step 5. support of application service

Ⅲ. 비교 및 검토

본 논문에서 제안 시스템과 기존 시스템 비교는 표 2와 같다.

표 2 기존 시스템과 제안 시스템 비교
Table 2 Comparison for proposed system and those of existing system

구분	기존 시스템	제안 시스템
인증대상	STB	STB, 콘텐츠 서버
암호알고리즘	대칭키	공개키, Session키
대역폭	낭비	절감
효율성	낮음	높음
인증 방식	단방향	양방향
스마트카드	필요	필요 없음
이동관리	어려움	쉬움
신분인증	스마트카드	ID, Password
CA시스템	ECM, EMM 기반 CA시스템 사용	공개키 기반 CA시스템 사용

기존 시스템은 사용자만 신분인증을 할 수 있다. 양방향전자상거래, 인터넷뱅킹, 전자문서 교환 등은 인증을 지원하지 못한다. 본 논문에서 제안한 시스템은 공개키를 사용하고, 사용자와 콘텐츠 서버를 인증을 통하여 IP 망에서 가로채기, 불법수정, 위조를 효율적으로 막을 수 있고 양방향전자상거래, 인터넷뱅킹, 전자문서 교환 등을 위한 안전한 플랫폼을 제공한다.

기존 시스템은 ECM을 모든 사용자에게 전송하기 때문에 대역폭을 낭비하다. 본 논문에서 제안한 시스템은 프로그램을 시청하는 사용자만 Sessionkey로 암호화된 콘텐츠를 전송받을 수 있고 대역폭을 절감하다.

디스크램블러와 스마트카드가 일체하기 때문에 기존 시스템은 STB를 옮기면 다시 설치해야한다. 본 논문에서 제안한 시스템은 스마트카드를 사용하지 않고 STB는 이동관리 쉽게 할 수 있다.

대칭키를 사용하는 기존 시스템은 안전을 위하여 복호화 알고리즘과 공개키를 주기적으로 갱신해야 한다. 공개키를 사용하는 제안 시스템은 개인키를 전송하지 않고 안전성을 향상시키다.

본 논문에서 제안한 시스템이 갖는 장점을 정리해 보면 다음과 같다. 첫째, 비싼 스마트카드 리더기를 STB내에 내장할 필요가 없어 비용 절감의 효과가 있다. 둘째, 디스크램블러와 스마트카드가 일체형이었던 기존의 방식과는 달리 디스크램블러와 가입자간의 독립성이 유지되므로 장소에 구애받지 않는다. 셋째, 공개키를 사용하여 안전적, 효율적인 인증 서비스를 제공할 수 있다.

Ⅳ. 결 론

전 세계에서 IPTV서비스의 급속한 확장을 통한 전자상거래, 인터넷뱅킹, 전자문서 교환 등에 대한 인증 문제가 매우 중요하다. 인증서는 개인 또는 기관에서 서명 및 암·복호화에 사용되는 공개키와 이에 대응 한 개인키의 소유 증명을 확인해 주는 전자문서로써 각 구성원의 신원을 증명하기 위한 중요한 수단이다.

본 논문에서는 가입자 편의를 위하여 스마트카드를 없애고 가입자 자신의 ID와 패스워드만 가지고 STB가 설치된 어떠한 장소에서도 IPTV 서비스가 가능한 새로운 PKI기반의 인증 수신 시스템을 제안하였다. 제안 시스템은 실시간 수신권한보호 강점 보이지만 개인정보보호와 PVR 불법 복제 방지에 취약점이 존재하다. 향후에는 공개키 기반 권한인증기능과 개인정보보호, 불법

복제 방지기능을 용합하는 시스템을 연구하는 것이 필요하다.

참고문헌

[1] ITU-T FG WG3,Working Document: IPTV Security Aspects, FG IPTV-DOC-0090Rev. 1, Geneva: IUT-T FG IPTV, July 22, 2007

[2] 원동호, "현대 암호학", 그린 출판사, 2004

[3] 최락권, 송치양, "IPTV서비스 구현을 위한 핵심 기술 연구", 전자공학회지 제35권 제3호, March 2008

[4] 이강석, 염홍열, 윤이중, "공개키 기반 구조 응용 분석 및 디지털 방송 한정 수신 시스템", 통신정보보호학회논문지 제8권 제3호, August 1998

[5] 최병선, 김상국, 채철주, 이재광, "모바일 단말기 상에서 안전한 인증을 위한 자바 기반의 PKI 시스템 연구", 정보처리학회논문지 C 제14-C권 제4호, August 2007

[6] 이장원, 홍기용, 조현숙, "스마트 카드를 이용한 네트워크 가입자 신분 확인", 한국정보 처리학회 논문지 제3권 제5호 September 1996

[7] 손종문, 김영민, "IPTV 셋톱박스 기술의 현황과 발전 방향", 정보처리학회지 제14권 제2호,March 2007

[8] 박종열, 문진영, 박민호, 백의현, "실시간 IPTV 서비스를 위한 수신 제한기술", 한국통신학회지, February 2007

저자소개

왕수(Wang Shuai)

2006년 곡부사범대학교 컴퓨터 과학기술학과(공학사)
2007년 ~현재: 배재대학교 컴퓨터공학과 석사과정
※관심분야:네트워크 보안, 프로그래밍 언어, IPTV

조인준(In-June Jo)

1982년 전남대학교 계산통계학과 (공학사)
1985년 전남대학교 전자계산학과 (공학석사)
1999년 아주대학교 컴퓨터공학과 (공학박사)
1983년~1994년 한국전자통신연구원 선임연구원
1994년~현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 정보보호, 컴퓨터 네트워크, 전산조직 응용