일반논문-09-14-3-02

# IPTV 방송 시스템에서의 속성기반 사용자 인증 기법

이 지 선[a], 김 효 동[b]‡

# Attribute-based authentication scheme in IPTV broadcasting system

Ji-Seon Lee[a] and Hyo Dong Kim[b]‡

요 약

IPTV(Internet Protocol Television)기술은 통신과 방송의 새로운 융합 기술로 다양한 양방향 TV 서비스를 제공한다. 이러한 서비스를 제공받기 위해서는 TV에 연결된 셋톱박스 (STB, Set-Top Box)와 정당한 가입자의 스마트카드 간의 상호 인증이 이루어져야 한다. 본 논문에서는 한 조직 내에서 직위나 부서 등과 같은 특성(속성) 값들에 따라, IPTV 서비스를 이용할 수 있도록 하는 속성기반 인증 기법을 제안하고, 제안하는 기법이 안전함을 보인다. 제안하는 기법에서 사용자는 자신의 아이디, 패스워드와 스마트카드를 이용하여 인증 메시지를 생성하는데, 이 때 자신에게 속한 다양한 속성을 이용할 수 있기 때문에 가입자는 한 번의 등록으로 속성에 따라 다양한 서비스를 제공받을 수 있다는 장점이 있다. 우리가 아는 한도 내에서는, 본 논문에서 제안하는 기법이 IPTV 환경이 조성된 어떤 조직에도 적용할 수 있는 최초의 속성인증 기법이다.

Abstract

An IPTV (Internet Protocol Television) technology is the new convergence technology of the telecommunication and broadcasting which provides various bidirectional TV services. To provide these services only to legal subscribers, mutual authentication between set-top box connected with TV set and the smart card owned by a subscriber is needed. In this paper, we propose an attribute-based mutual authentication scheme that only someone who is satisfied with some attributes, such as titles or departments, can access the contents provided by the IPTV service in an organization. We also show that the proposed scheme is secure. Our proposed scheme has a virtue that user can access various services, provided by an organization where he/she belongs to, according to their attributes with only one time registration. As far as we know, this is the first attribute-based authentication scheme which can be applied to any organizations in IPTV environments.

Keyword : IPTV, Set-top box, CAS, Smart card, Attribute-based authentication

## Ⅰ. 서 론

방송 콘텐츠가 디지털화되고 통신망이 광대역화 됨에 따라 다양한 양방향 TV 서비스를 제공하는 통합 융합의 새로운 서비스인 IPTV 서비스가 등장하게 되었다. IPTV 기술을 이용하면 기존의 방송 서비스와 같은 동영상 채널 서비스와 함께, PC 기반의 인터넷 및 데이터 서비스 등을 동시에 제공할 수 있다. IPTV는 이렇게 인터넷과 텔레비전의 융합이라는 점에서 디지털 컨버전스의 한 유형이라고 할 수 있는데, 기존의 인터넷 TV와 다른 점이라면 컴퓨터 모니터와 마우스 대신 TV 스크린과 리모콘을 사용한다는 것

a) 고려대학교 정보경영공학전문대학원 정보보호기술연구센터
Graduate School of Information Management & Security, CIST, Korea University
b) 아주대학교 미디어학부
Ajou University, Division of Digital Media
‡ 교신저자 : 김효동(hkim@commres.org)
· 접수일(2008년11월10일), 수정일(2009년4월8일), 게재확정일(2009년4월21일)

이다. 따라서 컴퓨터에 익숙하지 않은 사람이라도 TV 모니터와 리모콘을 이용하여 인터넷 검색, 홈쇼핑, 온라인 게임 등과 같은 인터넷이 제공하는 여러 서비스들을 제공받을 수 있다.

IPTV에서는 멀티캐스트 방식을 이용하여 방송 콘텐츠를 전송하는데, 이는 동일 네트워크에 다른 사용자가 있는 경우 하나의 전송으로 여러 명이 받아 볼 수 있도록 하는 방식이다. 이 때 중요한 것은 가입자 인증으로 동일 네트워크 상에서 가입되지 않은 사용자가 콘텐츠 내용에 접근하는 것을 막을 수 있어야 한다. 즉, 가입자 정보 기반의 채널 인증이 필요하다. 이러한 사용자 인증을 위해서 스마트카드가 이용되는데 스마트카드의 정보에 따라 TV에 연결된 셋톱박스(STB, Set-Top Box)는 인증 절차를 거친 후에, IP망을 통해서 멀티캐스트되는 스크램블된 콘텐츠 신호를 콘텐츠로 변환하여 TV 스크린에 보여주게 된다. 이때, 인증 절차는 STB 내에 존재하는 수신제한시스템(CAS, Conditional Access System)을 이용한다. 2004년에 Jiang et al.[1]에 의해서 처음으로 디지털 방송을 위한 STB와 스마트카드 간의 인증 기법이 제안되었고, 최근에는 Yoon과 Yoo[2]에 의해서 보다 안전한 인증 기법이 제안되었다.

이와 같은 인증방식이 중요한 역할을 하는 분야 중의 하나로 최근에 떠오르는 것이 사내방송의 구현이다. 즉, 기존의 IP망을 이용하기 때문에 새로운 방송망을 설치하는 부담이 줄어들어 많은 기업들이 사내방송 시스템으로 IPTV 기술을 많이 채택하고 있다. 이러한 IPTV 사내방송은 기존의 위성방송 기반 사내방송의 물리적 망의 한계를 극복하여 인터넷이 가능한 곳이면 어디서든 TV 혹은 컴퓨터를 통해 사내방송을 시청할 수 있는 것이 장점이며, 특히 별도의 네트워크를 구축할 필요 없이 기존의 인터넷 네트워크를 활용함으로써 비용절감의 효과가 있다. IPTV 기술을 활용함으로써 기업들의 사내방송이 단순히 회사의 소식을 회사 조직원 전체에게 전달하는 일방향적 수준에 그치는 것이 아니라, 특정 부서나 하부 조직의 특성화된 교육, 주요 임원들만이 공유할 수 있는 방송, 지역적으로 떨어져 있는 동종 부서 간의 커뮤니케이션과 행사 교류 등과 같은 다양한 커뮤니케이션 활동의 채널로 활용될 수 있게 된다[3-6].

이렇게 어떤 조직 내부에 IPTV 환경을 구축하여 세계 어디서나 자신이 속한 조직에서 제공되는 서비스를 이용할 수 있으려면 회사 구성원 외에 다른 사람은 회사 서비스에 접근할 수 없도록 해야 한다. 이 때, 직위나 부서 등과 같은 특성(속성) 값들에 따라, 제공되는 서비스의 종류를 달리 할 수 있다면 각 부서의 팀장만이 IPTV를 통해 장소에 관계없이 회의를 진행할 수 있도록 한다든가 혹은 특정 부서 소속원만이 특별한 교육을 받도록 할 수 있게 하는 등의 차등화된 작업을 할 수 있다. 사용자는 자신의 아이디, 패스워드와 가입자 관리 시스템으로부터 발급받은 스마트카드를 이용하여 인증 메시지를 생성하는데, 이 때 자신에게 속한 다양한 속성을 이용할 수 있기 때문에 가입자는 한 번의 등록으로 속성에 따라 다양한 서비스를 제공받을 수 있는 장점이 있다.

본 논문에서는 사내방송 환경과 같이 어떤 조직 내에서 각 개개인이 갖는 속성, 즉 사용자의 직위, 소속 등의 정보를 기반으로 하는 속성기반 인증 기법을 제안하는 것을 목적으로 한다. 논문에서 제시하는 속성기반 인증 기법은 인증의 다양성을 제공하기 위해 기존의 속성기반 암호화 기법[7]의 특성을 인증 프로토콜에 도입한 기법으로 논문의 구성은 다음과 같다. 우선 2장에서는 제안된 사내방송 시스템 구조와 인증을 위한 수신제한시스템에 대해 간략하게 서술하고, 3장에서는 보안 요구 사항과 속성기반 암호 시스템을 살펴본다. 4장에서는 새로운 속성기반 인증 기법을 제안하고 5장에서는 제안한 기법의 안전성에 대해 논한다. 마지막으로 6장에서는 결론을 맺는다.

## II. 사내 방송 시스템과 수신 제한 시스템

이번 장에서는 사내 방송 시스템의 구성도와 셋톱박스 내에서 인증을 담당하는 수신 제한 시스템을 살펴본다.

### 1. 사내 방송 시스템

사내방송 시스템은 미디어 콘텐츠를 제작하여 저장하여 두는 미디어 서버(Media Server)와 사내 방송 시스템 전체를 컨트롤하기 위한 강력한 중앙 제어 기능을 갖는 매니지

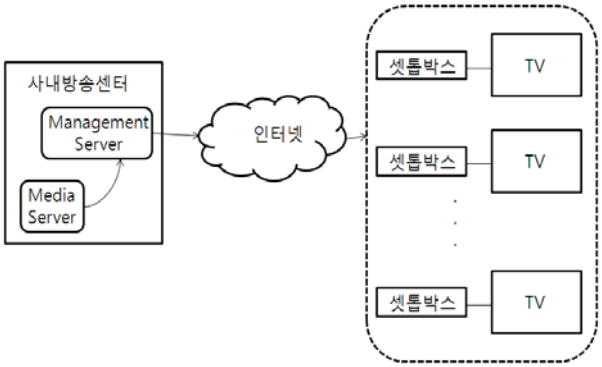


그림 1. 사내 방송 시스템 구성도
Fig. 1. Broadcasting System in Company

먼트 서버 (Management Server)를 중심으로 구성된다[그림 1]. 매니지먼트 서버의 주요 작업으로는 셋톱박스 관리, 콘텐츠의 등록 및 삭제, 특정 기간별로 예약 시간표의 작성 및 편집 등이 있다. 그리고 인터넷을 통하여 이 시스템에 접근할 수 있는 권한이 있는 사용자는 누구나 셋톱박스를 이용하여 사내 방송 센터에서 제공하는 콘텐츠를 볼 수 있다.

## 2. 수신제한시스템 (CAS, Conditional Access System)

IPTV 서비스 시스템에서는 정당한 가입자만이 콘텐츠를 볼 수 있도록 하는 기술인 수신제한시스템 (CAS, Control Access System)을 이용한다 [그림 2][8]. 수신제한 시스템은

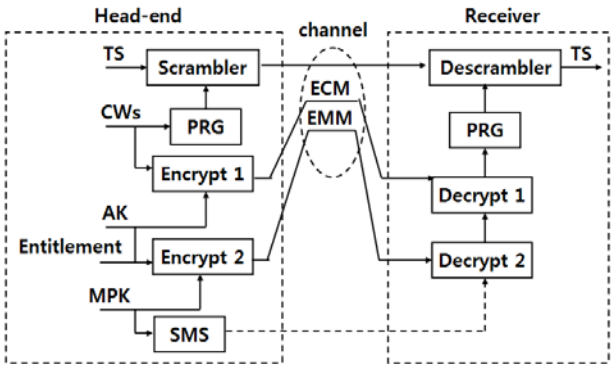


그림 2. 수신 제한 시스템
Fig. 2. CAS (Conditional Access System)

TV에 연결된 셋톱박스 내에 존재하는데, 셋톱박스는 서버 장비에서 송출하는 방송서비스 및 다양한 부가 서비스를 수신 및 재현하는 장치로 다양한 미디어 포맷 디코딩 기술, 콘텐츠 접근제어 기능, 양방향 데이터 방송 서비스 제공 등의 기능을 수행한다. 대개의 경우 셋톱박스는 두 개의 슬롯을 가지고 있는데, 첫 번째 슬롯은 프로그램 시청 권한을 체크하는 스마트카드를 위해 쓰이고, 두 번째 슬롯은 전자상거래를 목적으로 쓰인다. 스마트카드 리더는 반드시 ISO/IEC 7816-3 표준 규격을 따라야 한다.

사내 방송 센터에서는 미디어 콘텐츠를 스크램블링 (scrambling, 암호화)하여 전송하고, 이를 받은 수신자가 셋톱박스 내의 수신 제한 시스템을 이용하여 인증 확인 후 허가되면 디스크램블링(descrambling, 복호화) 과정을 통해 콘텐츠를 볼 수 있다. 이 때 스크램블링된 자료를 전송 스트림 (TS: Transport Stream)이라고 한다. 이러한 과정을 위하여 대부분의 시스템에서는 스크램블링하기 위한 키와 디스크램블링하기 위한 키로 동일한 키를 사용하는데 이를 제어 단어 (CW: Control Word)라고 한다. 사내 방송 센터에서는 보안을 위해 인증키 (AK: Authorization Key)를 이용하여 제어 단어를 암호화하여 자격 제어 메시지 (ECM: Entitlement Control Message)를 통해 전송한다. 인증키는 다시 가입자 비밀키 (MPK: Master Private Key)를 사용해서 암호화한 뒤에 자격 관리 메시지 (EMM: Entitlement Management Message)를 통해 전송한다. 즉, 보안을 위하여 전송 스트림 외에 자격 제어 메시지와 자격 관리 메시지가 같이 전송된다. 이 때 가입자 비밀키를 관리하는 것은 가입자 관리 시스템(SMS, Subscriber Management System)이고 가입자 관리 시스템이 관리하는 자료를 가지고 자격 관리 메시지와 자격 제어 메시지를 생성하여 신규 가입자가 가입한 방송 채널을 수신하거나 탈퇴한 가입자가 더 이상 방송을 수신하지 못하도록 하는 것은 가입자 인증 시스템(SAS, Subscriber Authorization System)이다.

수신기에서 전송 스트림, 자격 제어 메시지와 자격 관리 메시지를 받으면 서버가 이용한 가입자 비밀키를 알아 내어 전송 스트림을 복호화하여 원하는 서비스를 이용하게 된다. 이 때 일반적으로 가입자 비밀키는 가입자가 최초로 가입하는 시점에 가입자 관리 시스템에 의해 관련 비밀 정

보들과 함께 스마트 카드 안에 내장되어 가입자에게 배포된다. 스마트카드와 셋톱박스는 안전하게 제어 단어를 주고받기 위하여 공유키를 생성하고, 스마트카드는 우선 내장된 가입자 비밀키로 제어 단어를 복호화해 낸다. 다음으로 스마트카드는 생성한 공유키로 제어 단어를 암호화하여 셋톱박스로 보낸다. 암호화된 제어 단어를 받은 셋톱박스는 공유키로 제어 단어를 복호하여 전송스트림을 디스크램블링하고 콘텐츠를 가입자에게 보여준다.

따라서 정당한 가입자만이 콘텐츠를 볼 수 있도록 하기 위해서는 스마트카드와 셋톱박스 간의 상호 인증이 필요하고, 제어 단어를 안전하게 전달하기 위하여 둘 간에 공유키를 생성하는 것이 중요하다.

## III. 관련 연구

이번 장에서는 셋톱박스와 스마트카드 간의 인증 과정에서 필요로 하는 보안 요구 사항과 속성기반 암호 시스템을 살펴본다.

### 1. 보안 요구 사항

스마트카드와 셋톱박스 사이에 가능한 공격 기법으로는 다음과 같이 맥코맥 핵 공격 (McCormac Hack Attack)과 스마트카드 복제 공격 (Smart Card Cloning Attack)이 있는데 이 두 공격은 모두 정당하지 않은 스마트카드를 셋톱박스가 정당한 스마트카드로 인지하도록 하려는 공격이다[9].

- 맥코맥 핵 공격 (McCormac Hack Attack) : 스마트카드로부터 셋톱박스로 연결되는 데이터 라인을 같은 종류의 다른 셋톱박스로 전송하여 접근허가를 받으려는 공격이다.
- 스마트카드 복제 공격 (Smart Card Cloning Attack) : 정당한 스마트카드를 복제하여 복제된 카드를 다른 셋톱박스에 넣어서 접근허가를 받으려는 공격이다.

디지털 방송 환경에서 셋톱박스와 스마트카드 간의 인증은 일반적인 인터넷을 통한 서버-클라이언트 인증과는 여러 면에서 다르게 구현되어야 한다. 인터넷을 통한 서버-클라이언트 인증 기법에서는 둘 사이에 주고 받는 데이터가 인터넷을 통하여 전달되기 때문에 인터넷 보안 문제 - 예를 들어, 인터넷 상의 데이터를 가로채서 변형하여 전달하는 공격 등 - 를 반드시 고려해야 하지만, 셋톱박스와 스마트카드 간의 인증에서는 둘 사이에 전달되는 데이터가 셋톱박스 내에서 전달되기 때문에 위에서 언급한 맥코맥 핵 공격과 스마트카드 복제 공격에 안전함을 보이는 것이 가장 중요한 고려사항이다.

### 2. 속성기반 암호 (ABE : Attribute-Based Encryption)

일반적으로 속성은 특징을 표시하며, 주어진 데이터를 정의하고 설명한다. 큰 집합 내에서 사용될 때에는 비슷한 대상들의 효율적인 분류를 가능하게 해준다. 예를 들어, 기업 내에서 개인은 속성 값에 기반하여 공통의 관심이나 업무로 분류될 수 있다. 2005년 Sahai와 Waters에 의해 처음 제안된 속성기반 암호 시스템은 개인이 소유한 속성 값들을 기반으로 각 개인에 대하여 특정 파일이나 특정 업무에 대한 정보에 접근 허가 여부를 판단할 수 있도록 하는 암호 시스템이다[7]. 이는 기존의 신원(identity) 기반 암호 시스템을 일반화한 것으로 속성 값을 암호 인자로 사용하여 속성에 대한 비밀 키를 가지고 있는 사용자만이 암호화된 데이터를 복호할 수 있도록 제안된 암호화 기법이다. 즉, 메시지는 의도된 수신자를 설명하는 일련의 속성 값을 이용하여 암호화 되며, 이때 이용된 속성 값을 소유한 사람만이 원래 메시지를 복호할 수 있도록 한다. 이러한 속성기반 시스템은 분산 환경에서 데이터의 안전성을 제공할 수 있는 암호 기법으로 높이 평가받고 있다. 이러한 속성 기반 시스템에 기반하여 최근에 Rhee et al.은 익명성을 보장하는 속성기반 사용자 인증 기법을 제안하였다[10].

## IV. 셋톱박스와 스마트카드 간의 속성 인증 기법

이번 장에서는 속성기반 인증 기법을 제안한다. 제안하

는 기법은 등록 단계, 로그인 단계, 그리고 상호 인증 단계, 제어 단어 전달 단계로 이루어진다. 등록 단계에서는 새로운 가입자가 가입자 관리 시스템으로부터 자신의 속성과 비밀 정보 등을 갖는 스마트카드를 발급받는다. 각 가입자는 자신에 해당하는 여러 속성들을 갖고, 특정 콘텐츠에 접근하고자 할 때에는 자신의 모든 속성이 인증과정에 필요할 수도 있지만, 자신의 속성 일부분만이 만족되는 경우에도 콘텐츠 접근이 허용되어야 한다.

우선적으로 가입자 관리 시스템은 각 속성 값별로 제공받을 수 있는 서비스에 대한 정의를 내리는 것이 필요하다. 각 사용자는 서버가 제공할 수 있는 서비스를 확인한 후 자신의 개인 정보를 이용하여 서버에 미리 등록한다. 이때 서버는 사용자가 가지고 있는 자격 (소속 부서, 직급 등)을 인증하고 사용자에게 제공할 수 있는 서비스에 해당하는 특성 값을 제공하게 된다. 사용자는 자신에게 발급된 특성 값들을 이용하여 그때그때 필요한 서비스를 요청하게 된다. 가입자 관리 시스템은 $U_i$가 입력한 정보(이름, 사번, 주민번호 등)를 바탕으로 $U_i$의 속성 (해당 부서, 직급 등의 정보)을 확인하고 $U_i$의 속성 집합 $A_i = \{a_{i,1}, a_{i,2}, ..., a_{i,n}\}$을 결정한다.

본 논문에서 제안하는 기법에서는 다음의 용어들을 사용한다.

- $ID_i$, $PW_i$: 사용자 $U_i$의 아이디, 패스워드
- $ID_S$ : 셋톱박스의 고유 일련 번호 (셋톱박스의 아이디)
- $x_S$ : 셋톱박스의 비밀키
- $l$ : 보안 파라미터
- $p$ : 임의의 큰 소수
- $h(\bullet): \{0,1\}^* \rightarrow \{0,1\}^l$ : 일방향 해쉬 함수
- $\oplus$ : bitwise exclusive-or 연산자
- $A_i = \{a_{i,1}, a_{i,2}, ..., a_{i,n}\}$ : 사용자 $U_i$에 대한 모든 속성 집합
- MPK : 가입자 비밀키

가입자의 모든 속성을 $A_i = \{a_{i,1}, a_{i,2}, ..., a_{i,n}\}$라고 할 때, $A_i$의 모든 원소가 인증 과정에 필요할 수도 있고, 콘텐츠에 따라서는 $A_i$의 속성 중 일부 $\{a_{i,1}, a_{i,2}, ..., a_{i,k}\} \subseteq A_i (k \leq n)$만을 셋톱박스가 요구하는 경우에도 인증되어야 한다. 여기에서 $k$ 개의 속성은 전체 $n$ 개의 속성 중에서 임의로 선택된 것을 나타낸다. 즉, $a_{i,j} \in A_i (1 \leq j \leq k)$ 이다.

**<등록 단계>**

1. 새로운 가입자 $U_i$가 스마트카드를 발행받기 위해서 자신에 대한 정보(이름, 사번, 주민번호 등)과 자신이 선택한 아이디 $ID_i$와 암호 $PW_i$를 가입자 관리 시스템에 보낸다.
2. 가입자 관리 시스템은 $U_i$가 입력한 정보(이름, 사번, 주민 번호 등)를 바탕으로 $U_i$의 속성 (해당 부서, 직급 등의 정보)을 확인하고 $U_i$의 속성 집합 $A_i = \{a_{i,1}, a_{i,2}, ..., a_{i,n}\}$을 결정한다.
3. 가입자 관리 시스템은 다음과 같이 $x_{i,j} (1 \leq j \leq n)$를 계산한다. 여기에서 $x_S$는 셋톱박스의 비밀키이다.

$$x_{i,j} = h(ID_i, PW_i) \oplus h(a_{i,j} \oplus x_S), \ (1 \leq j \leq n)$$

4. 가입자 관리 시스템은 임의의 정수 $y_i$를 선택하고 다음을 계산한다.

$$IDPW_i = h(ID_i, PW_i) \oplus y_i$$

$$f(x) = \prod_{j=1}^{n} (x - x_{i,j}) + y_i$$

$$h_{i,j} = h(a_{i,j} \oplus PW_i) \oplus x_{i,j}, \ (1 \leq j \leq n)$$

$$H_i = \{h_{i,1}, ..., h_{i,n}\}$$

$$X_i = \{x_{i,1}, \ ... \ , x_{i,n}\}$$

5. 가입자 관리 시스템은 스마트카드에 $\{IDPW_i, A_i, f(x), H_i, X_i, h(ID_s), h(\bullet), MPK\}$을 저장하여 $U_i$에게 보낸다.

**<로그인 단계>**

가입자가 자신이 원하는 콘텐츠를 받아 보기 위해서는

해당 콘텐츠를 받아볼 수 있는 속성 정보들을 가지고 있어야 한다. (제공되는 콘텐츠들은 각각의 콘텐츠에 접근하기 위한 속성 정보들을 미리 가지고 있다고 가정한다.)

1. 가입자 $U_i$는 자신의 아이디 $ID_i$와 암호 $PW_i$, 그리고 해당 콘텐츠를 보기 위해 $n$개의 속성 중에서 필요한 $k$개의 속성들을 선택하여 보낸다 $(k \le n)$. 여기서 $k$개의 속성은 전체 $n$개의 속성 중에서 선택된 것이지만, 표기의 편의상 $k$개의 속성을 $\{a_{i,1}, a_{i,2}, ..., a_{i,k}\}$로 표기한다.
2. 스마트카드는 $U_i$로부터 입력받은 정보가 정당한 가입자 정보인지를 다음과 같이 확인한다.
   (1) $x_{i,j}' = h_{i,j} \oplus h(a_{i,j} \oplus PW_i)$, $(1 \le j \le k)$, 와 $y_{i,j}' = f(x_{i,j}')$를 계산한다. 이 때 계산된 $k$개의 $y_{i,j}'$ 값은 모두 같아야 한다. 만일 같지 않다면, 로그인 요청을 거절한다.
   (2) 위에서 계산된 $k$개의 $y_{i,j}'$ 값이 모두 같다면, 모든 $j$ $(1 \le j \le k)$에 대해서 입력받은 $ID_i$와 암호 $PW_i$를 이용하여 다음 등식이 성립하는지를 검증한다. 로그인 요청을 받아들였다면, $y_{i,j}'$는 모두 같은 값이므로 $y_i'$라고 표기하겠다. 셋톱박스가 요구하는 $k$개의 속성에 대해서 다음의 등식이 성립하면 스마트카드는 $U_i$의 로그인 요청을 받아들인다.

$$IDPW_i \oplus y_i' = h(ID_i, PW_i)$$

**<상호인증 단계>**

1. 모든 $k$개의 속성 값들 $\{a_{i,1}, a_{i,2}, ..., a_{i,k}\}$에 대한 사용자 $U_i$ 의 인증이 성공하면 스마트카드는 임의의 난수 $r \in Z_p^*$을 선택하여 다음과 같이 $Y$ 값을 계산하여 속성 값들 $\{a_{i,1}, a_{i,2}, ..., a_{i,k}\}$과 같이 셋톱박스에 보낸다.

$$H = \prod_{j=1}^{k} (x_{i,j}' \oplus h(ID_i, PW_i))$$
$$Y = H \oplus r$$

2. 셋톱박스는 스마트카드로부터 받은 $Y$와 속성값 $\{a_{i,1}, a_{i,2}, ..., a_{i,k}\}$을 가지고 임의의 정수 $r' \in Z_p^*$을 선택하여 다음을 계산한다. 그리고 스마트카드로 $(R_1, R_2)$를 보낸다.

$$H = \prod_{j=1}^{k} h(a_{i,j} \oplus x_S)$$
$$r = H \oplus Y$$
$$R_1 = h(r, h(ID_S)) \oplus r'$$
$$R_2 = h(r, r')$$

3. $(R_1, R_2)$를 받은 스마트카드는 $r' = R_1 \oplus h(r, h(ID_S))$을 계산한 후, $R_2$와 $h(r, r')$ 값이 같은지 비교하여 두 값이 같으면 셋톱박스를 인증하고 $R_3 = h(r', r)$를 셋톱박스로 보낸다.
4. 셋톱박스는 $R_3$가 $h(r', r)$와 같은지 비교하여, 만약에 같다면 셋톱박스는 스마트카드를 인증한다.

**<제어 단어 전달 단계>**

1. 스마트카드와 셋톱박스의 상호 인증이 성공하면, $SK = h(ID_i, h(ID_S), r, r')$를 공유키로 사용한다.
2. 스마트카드는 가입자 비밀키 $MPK$를 이용하여 제어 단어를 복호화해내고, 계산한 공유키 $SK$를 이용하여 제어 단어를 암호화하여 셋톱박스에 보낸다.
3. 셋톱박스는 암호화된 제어 단어를 공유키 $SK$를 이용하여 복호화해서 원하는 콘텐츠를 디스크램블링한다.

## Ⅴ. 보안 요구 분석

이번 장에서는 위에서 제안한 기법이 다음과 같은 보안 요구를 만족함을 보인다.

(1) 맥코맥 핵 공격에 대한 안전성 : 우리가 제안한 기법에서 스마트카드는 셋톱박스의 고유 번호는 모르지만 그것의 해쉬값 $h(ID_S)$를 저장하고 있다. 이 값은 각 셋톱박스의 유일한 식별자이기 때문에 다른 식별자를

갖는 셋톱박스와는 인증이 불가능하다. 즉, 스마트카드로부터 셋톱박스로 전달되는 데이터들을 다른 셋톱박스로 전달한다고 하더라도 스마트카드가 가지고 상대 셋톱박스의 고유번호의 해쉬값이 틀리기 때문에 상호 인증을 불가능하다. 따라서 우리의 기법은 맥코맥 핵 공격에 안전하다.

(2) 스마트카드 복제 공격에 대한 안전성 : 스마트카드 복제 공격에서는 각 셋톱박스가 유일한 식별자에 대한 해쉬값 $h(ID_S)$, 셋톱박스만의 비밀키 $x_S$를 가지므로 다른 식별자와 비밀키를 갖는 셋톱박스에 복제된 스마트카드를 넣더라도 인증이 불가능하다.

## Ⅵ. 결 론

본 논문에서는 인터넷 프로토콜에 기반을 둔 사내 방송 시스템에서 속성에 따라 사내 콘텐츠에 접근할 수 있는 권한을 제한할 수 있는 속성기반 인증 기법을 제안하였다. 사용자는 자신의 아이디, 패스워드와 가입자 관리 시스템으로부터 발급받은 스마트카드를 이용하여 인증 메시지를 생성하는데, 이 때 자신에게 속한 다양한 속성을 이용할 수 있기 때문에 가입자는 한 번의 등록으로 속성에 따라 다양한 서비스를 제공받을 수 있는 장점이 있다. 우리가 아는 한도 내에서는 우리의 기법이 스마트카드와 셋톱박스 간에 속성을 기준으로 한 최초의 인증 기법으로 사내 방송 시스템에서와 같이 여러 다양한 속성을 가진 사람들로 구성된 조직에서 유용한 기법이다.

## 참 고 문 헌


[1] T. Jiang, Y. Hou, and S. Zheng, “Secure communication between set-top box and smart card in DTV broadcasting,” IEEE Trans. On Consumer Electronics, Vol. 50, No. 3, August, 2004, pp.882-886.

[2] E.-J. Yoon and K.-Y. Yoo, “Robust key exchange protocol between set-top box and smart card in DTV broadcasting,” INFORMATICA, Vol. 20, No. 1, 2009, pp.139-150.

[3] 김재철, “삼성네트웍스, 삼성그룹 내 IPTV 방송망 구축한다”, 전자엔지니어, 2006. 11. 3.

[4] 임지수, “KT, 사내방송 IPTV 방식으로 전환”, 전자신문, 2007. 11. 6.

[5] 홍기범, “IPTV 바람 타고 사내방송 관련업계 활기", 전자신문, 2008. 10. 13.

[6] 박형수, “리노스, 한국도로공사와 6.6억 규모 계약 체결”, 아시아경제, 2008. 10. 31.

[7] A. Sahai and B. Waters, “Fuzzy identity based encryption," Proc. of Eurocrypt'05, LNCS 3494, 2005, pp. 457-473.

[8] F. Kamperman and B.V. Rijnsoever, “Conditional access system interoperability through software downloading,” IEEE Trans. On Consumer Electronics, Vol. 47, No.1, 2001, pp.47-53.

[9] W. Kanjanarin and T. Amornraksa, “Scrambling and key distribution scheme for digital television,” IEEE International Conference on Networks, Oct. 2001, pp.140-145.

[10] 이현숙, 유혜정, “스마트카드를 이용한 속성기반 사용자 인증 스킴,” 정보보호학회논문지, 제18권 제5호, 2008. 10.


## 저 자 소 개


이 지 선

- 1991년 : 서강대학교 전자계산학과 졸업 (학사)
- 1998년 : 서강대학교 컴퓨터공학과 졸업 (석사)
- 2008년 : 서강대학교 컴퓨터공학과 졸업 (박사)
- 2008년 ~ 현재 : 고려대학교, BK21 유비쿼터스 정보보호 사업단 연구교수
- 주관심분야 : 암호학, 네트워크 보안, 무선통신 보안, IPTV 보안

## 저 자 소 개


### 김 효 동

- 1992년 : 서강대학교 사학과 졸업(학사)
- 1997년 : University of Utah, Communications 졸업 (석사)
- 2003년 : Rutgers University, Communications 졸업 (박사)
- 2004년 ~ 현재 : 아주대학교 미디어학부 부교수
- 주관심분야 : 커뮤니케이션 테크놀로지, 디지털방송