# Single-Sign-On을 이용한 IPTV 사용자 인증방안

김 강$^{O}$ ,정종일, 송상훈, 신동규, 신동일
세종대학교 컴퓨터공학과
{kimkang$^{O}$, jijeong, song, shindk, dshin}@gce.sejong.ac.kr

# IPTV User Authentication using Single-Sign-On

Kang Kim$^{O}$ J.I. Jeong, S.H. Song D.K. Shin D.I. Shin J.I
Dept of Computer Engineering, Sejong University

**요 약**

DTV는 방송 서비스 운영에 가입자 개념을 추가하여 무료방송 외에 정당한 수신료를 지불하는 사람만이 프로그램을 시청할 수 있도록 하며, 그러한 수익을 이용하여 보다 양질의 서비스를 제공할 수 있게 되었다. 가입자간의 구분을 가능하게 해주기 위한 방법이 제한수신시스템(CAS: Conditional Access System)이다. IPTV는 웹 브라우저를 기반으로 동작하며, 방송 콘텐츠라는 기본 TV기능에서 벗어나 T-commerce, E-commerce 등의 다른 도메인으로 사용자의 요구에 따라 자유롭게 이동하며 사용자인증이 요구되기 때문에 기존의 제한수신시스템으로는 그 기능을 다 하기 힘들어졌다. Single-Sign-On은 사용자가 단한 번의 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 사용자인증의 번거로움을 해결할 수 있는 편의성을 제공하는 SSO의 융합은 필연적이라 할 수 있다. 그러므로 Single-Sign-On은 사용자의 요구에 따라 이동하기 쉬운 IPTV 환경에 매우 적합하다. 이 논문에서는 제한수신시스템, SSO, IPTV에 대해 설명하고 제한수신시스템과 SSO의 기능을 통합하여 IPTV환경에 적합한 새로운 인증방안을 제안한다.

## 1. 서 론

위성과 케이블 망 등을 이용한 디지털 방송의 시대에 가입자는 개별화되고 전문화된 채널 서비스를 받을 수 있고, 방송 사업자는 기존의 광고료 수입에만 의존하던 서비스를 탈피하고 방송 서비스 운영에 가입자 개념을 추가하여 무료방송 외에 정당한 수신료를 지불하는 사람만이 프로그램을 시청할 수 있도록 하며, 그러한 수익을 이용하여 보다 양질의 서비스를 제공할 수 있게 되었다. 이러한 가입자간의 구분을 가능하게 해주기 위한 방법이 제한수신시스템(CAS: Conditional Access System)이다. 하지만 기존의 디지털방송보다 더 확장된 개념인 IPTV의 등장으로 제한수신시스템만으로는 그 기능을 다 하기 힘들어졌다. IPTV는 인터넷을 기반으로 하는 양방향 통신을 기반으로 하여 필요시에는 웹브라우저로 화면을 전환하여 다른 서비스를 이용하며, E-commerce와 T-commerce등 사용하는 서비스에 따라 재차 로그인(인증)이 필요하기 때문에 그로인해 사용자의 불편을 유발하고, 서비스 제공자는 해당 콘텐츠로의 사용자 접근 저하를 우려 할 수 있기 때문이다.

본 논문에서는 유료 서비스를 위한 제한수신시스템의 구조와 기능, 제한수신시스템의 보호메커니즘에서 인증에 대해 살펴보고, Single-Sign-On(SSO)의 개념을 알아본 후, 제한수신시스템과 SSO를 접목시켜 IPTV시대를 대비하여 사용자 인증의 편의성 증진을 위한 방안을 제안한다.

## 2. Conditional Access System (CAS)

디지털 방송에서 정당한 가입자만이 콘텐츠에 대한 접근이 허용되어야 하며, 이러한 제한수신시스템[2]은 가장 중요한 요소 중 하나이다. 본 장에서는 제한수신모델의 구조와 기능에 대해 기술한다.

제한수신시스템이란 각 단말기에 방송 프로그램을 시청할 수 있는 권한을 부여하거나 제한하는 시스템이다. 유료방송에서는 방송사에서 방송 콘텐츠를 암호화된 신호로 위성 · 지상파 · 케이블 등을 통해 전송하고, 요금을 지불한 시청자의 단말기에만 암호를 풀 수 있는 권한을 부여해 시청할 수 있도록 구현한 시스템이다.

제한수신시스템은 첫째로, 시청료를 지불한 정당한 가입자만이 프로그램을 시청할 수 있도록 신분확인(authentication)과 접근제어(access control)가 가능해야 하며, 둘째로 통신 연결 상태에서의 모든 데이터는 미가입자의 불법 도/시청을 막을 수 있어야 한다. 이와 같이 가입자와 자원(데이터, 프로그램)을 보호하기 위한 것으로는 사용자인증방안, 스크램블링/디스크램블링 이 있다.

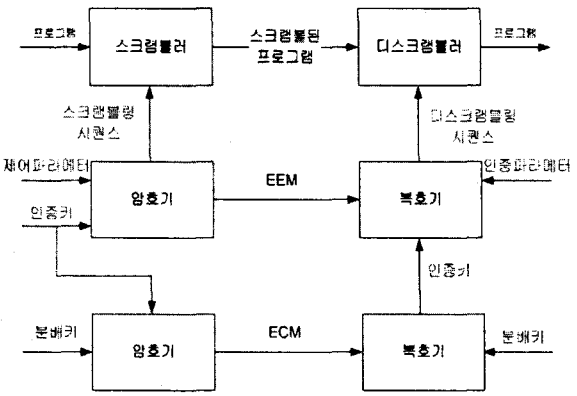


그림 1 Conditional Access System

방송망에 적용되는 제한수신기술[4]은 크게 스크램블러(scrambler)의 제어단어(CW: Control Word)를 분배하는 기능과 제어단어를 암호화하여 전달하는데 사용되는 인증키(AK: Authentication Key)를 분배하는 기능, 그리고 스크램블링/디스크램블링 기능으로 분류된다. 제어단어를 인증키를 통하여 암호화하여 수신자 측에 전달하는 메시지를 자격통제메세지(ECM: Entitlement Control Message)라고 하고, 인증키를 전달하기 위한 메시지를 (EMM : Entitlement Management Message)라고 한다. (그림 1)은 제한수신시스템의 일반적 구성을 보여준다. 스크램블링/디스크램블링에 의해 콘텐츠를 직접 보호하고, 제어워드(CW : Control Word)를 가진 수신기들에서만 프로그램을 디스크램블링하여 시청이 가능하도록 분배하며, 제어워드를 암호화하여 전달하는데 이용되는 인증키 (AK: Authentication Key)를 분배 하는 기능을 갖추고 있다.

프로그램을 디스크램블하기 위해 필요한 권한과 관련 키들을 자격(Entitlement)이라 한다. 이 기능은 난수 발생의 초기치인 제어워드를 암호화하고 그 제어워드를 자격통제메세지 (ECM : Entitlement Control Message)를 통해 전송한다.

수신기는 자격통제메시지를 받게 되면 스마트카드라고 하는 보안 장비로 메시지를 보내어 합당한 데이터인지를 체크한 후 제어워드를 복호화 하여 디스크램블러로 보내게 되고, 올바른 가입자는 원하는 프로그램을 시청할 수 있다.

자격통제메시지에는 암호화된 제어워드 외에 프로그램 정보와 접근 파라미터도 함께 전송된다.

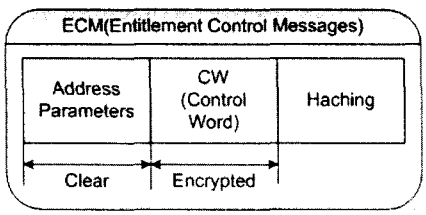


그림 2 Entitlement Control Messages

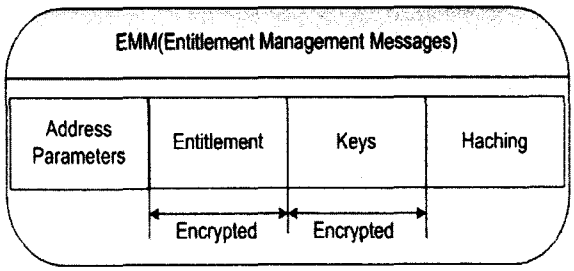


그림 3 Entitlement Management Messages

제어단어를 인증키(AK)로 암호화하여 방송수신측에 전달하며, 모든 수신기는 수신한 자격통제메시지에 포함된 제어워드와 접근 파라미터를 수신기와 접속된 스마트카드에 전달하여 프로그램 취득 조건 및 자격을 심사한 후 정당한 프로그램으로 판단이 되면, 스마트 카드내의 서비스키를 이용하여 제어단어를 해독하고 디스크램블하여 합법적인 소비자에게 제공한다.

## 3. Single-Sign-On (SSO)

Single-Sign-On[1]은 사용자가 단한번의 인증(or 로그인)을 통하여 추가적으로 인증할 필요가 있는 다른 서비스로의 자동적인 인증을 제공한다. 그러므로 Single-Sign-On은 사용자의 요구에 따라 이동하기 쉬운 Web Service 환경에 매우 적합하다. 개인의 경우, 사이트에 접속하기 위하여 아이디와 패스워드는 물론 이름·전화번호 등 개인정보를 각 사이트마다 일일이 기록해야 하던 것을 한 번의 작업으로 끝나므로 불편함이 해소되며, 기업에서는 회원에 대한 통합관리가 가능해 마케팅을 극대화시킬 수 있다는 장점이 있다.

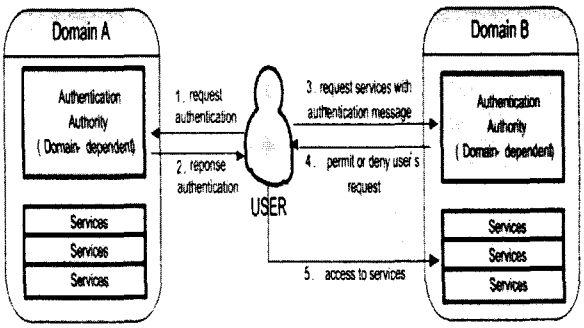


그림 4 Single-Sign-On

(그림4)와 같은 SSO방식은 도메인에 독립적인 분산처리 서비스 환경에 유용하다. 사용자가 많은 도메인으로의 접근을 원할 때 각 도메인은 사용자인증을 요청하게 된다. 이 경우 사용자는 하나의Domain에 의해 인증되고 그 정보는 SOAP message에 결속된다. 이런 경우 다른 도메인에서 사용자에게 직접적으로 인증정보 제공을 요청할 필요가 없다.

[표1] Comparison of Single Sign-On implementation methods

| Approach | Method | Kind of security token |
|---|---|---|
| Central repository | Passport | |
| | Liberty Alliance | |
| Message attachment | Keberos | Keberos ticket |
| | WS-Security | X.509 certificate, Keberos ticket, username/password |
| | SAML | Keberos ticket, Password, Name Identifier (application defined), various of keys, Secure Remote Password (SRP), Hardware token, SSL/TLS Certificate Based Client Authentication, X.509 public key, PGP public key, SPIK Public key, XML Digital Signature, Unspecified |

## 4. IPTV의 개념과 서비스 유형

IPTV(Internet Protocol TV)란 통신사업자 입장에서 기존의 통신 서비스 기반 위에서 비디오 서비스를 제공하며, 좁은 의미에서는 Walled Garden, VOD 등 초고속 인터넷 부가 서비스로 서비스 제공영역을 PC에서 TV로 확장시킨 개념이지만, 넓은 의미로는 초고속 인터넷망을 방송매체로 활용하여 Audio/Video 형태의 방송채널을 적극적으로 수용하는 것을 포함한다. 인터넷에 접속하여 디지털 정보를 주고받는 TV이기 때문에 T-commerce등의 전자상거래를 효율적으로 활용할 수 있다.

IPTV는 초고속 인터넷과 DTV의 기능을 묶은, 통방융합의 새로운 트렌드로 떠오르고 있다. 기존 TV 기기와 인터넷 모뎀을 연결하여 인터넷과 방송 서비스를 제공함으로써 방송에는 익숙하지만 PC환경에는 다소 미숙한 세대에 대한 새로운 서비스를 제공할 수 있으며, 인터넷 다운로드나 방송 등의 기술과 달리 기존 네트워크 인프라와 인터넷을 사용하여 많은 수의 사용자가 이용가능하다. 최근에는 기술적으로 셋톱박스(STB) 안에 인터넷 모뎀의 기능이 결합하여 지능형 통합 셋톱박스 화하는 추세로 변화하면서 홈 네트워크라는 차세대 댁내 네트워크 서비스를 제공하기 위한 전략적 단말로서 위치가 커져가고 있다.

IPTV는 일반적인 기본형 채널(SD/HD영상, Audio)뿐만 아니라 다음과 같은 선택형 맞춤 채널과 양방향 데이터 서비스를 제공한다.

- T-info
  날씨, 뉴스, 생활정보, 교통정보, 지역정보
- T-Commerce
  증권, 쇼핑, 뱅킹, 경매, 장터, 주문배달
- T-Com.
  SMS, 메신저, 메일, 채널채팅, 영상전화
- T-entertainment
  블로그, 사진, 게임, 모바일
- T-learning
  영유아, 초중고, 어학

## 5. IPTV를 위한 Single Sign-On 인증

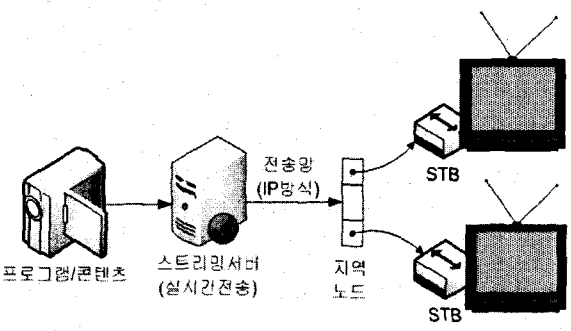


그림 5 IPTV 개념도

### 5.1 Single-Sign-On 구현 방식

[표1]은 SSO를 실행하기 위한 2개의 대표적인 구현방식을 보여준다. 첫 번째 방식은 모든 사용자 인증 정보를 1개의 저장소에서 보관하고, 두 번째 방식은 사용자 인증 정보를 각 도메인에서 보관한다.

Passport와 Liberty Alliance는 중앙저장소(Central repository)를 채용하고 있는 방법이다. 마이크로소프트가 개발하는 Passport에서, 사용자는 Microsoft에의해 관리되는 Passport 서버에 가입하고, 그것에 의해 인증을 받는다. Liberty Alliance는 연합을 이룬 network ID management에 의해 ID에 기반을 두는 서비스 표준을 정의한다.

Keberos, WS-Security와 SAML은 메시지첨부(Message attachment)방식을 채용하여 웹서비스메세지에 인증정보를 담는다. 티켓(ticket)에 기반한 Keberos는 Soap message에 티켓을 첨부하여, 사용자인증 정보가 중간매개체를 통해 최종 도메인에 전달된다. WS-Security는 웹서비스메세지에 완전성과 신뢰성을 반영하기 위해 정의되었다. SAML은 OASIS(Organization for Advancement of Structured Information Standard)

에서 권장하는, 보안 토큰의 유형을 정의하고 토큰을 포함하여 웹기반의 Single-Sign-On을 실행하기 위한 표준이다.

첫 번째 중앙저장소 방식은 사용자의 기존 ID를 삭제하고 중앙저장소로부터 새로운 ID를 할당 받고, 서비스에 접근할 때 새로운 ID를 사용해야 한다. 이 접근방식은 단일도메인 서비스를 위한 구성에 적합하다. 모든 사용자의 정보가 중앙저장소로 저장되기 때문에 각 도메인의 보안정책은 중앙저장소를 따라야 하고 사용자정보에 대한 제어가 어려워진다. 또한 이 접근방식은 확장성을 기대하기도 힘들고, IPTV의 분산서비스 환경에 적합하지 않다.

두 번째 메시지첨부 방식은 다양한 보안 토큰을 이용하여, 사용자의 최초 접근 시에만 인증을 받으면 다른 도메인이나 서비스로 이동시에 추가적인 작업 없이 사용자 인증이 가능하고, 티켓 등의 암호화된 정보를 주고받기 때문에 공개되어 있는 네트워크 환경에서 보안성이 우수하여, 빈번한 서비스 이동이 예상되는 IPTV환경에서 첫 번째 방식보다 보안상이나 사용자 편의상 월등한 성능을 보여준다.

### 5.2 Single Sign-On의 IPTV적용

기존의 DTV환경에서의 제한수신시스템은 방송 서비스 제공자의 입장에서 유료 콘텐츠에 대한 올바른 사용자를 구분하고 양질의 서비스를 제공하기 위해 사용되었다. 하지만 양방향 분산 서비스를 기반으로 하고 웹 브라우저를 사용하는 IPTV는 DTV의 기본적 서비스 외에도 서로 다른 도메인 내 서비스간의 전환이 매우 자유롭고, 전자상거래와 같이 사용자 인증이 요청되는 상황이 빈번하게 나타난다. 소수의 제공자와 다수의 사용자가 정보를 주고받는 DTV와는 달리, 다수의 사용자가 다수의 서비스를 제공받기를 원하는 IPTV환경에서는 단순한 사용자 인증과 접근제어의 기능을 가진 제한수신시스템과 빈번한 사용자인증의 번거로움을 해결할 수 있는 편의성을 제공하는 SSO의 융합은 필연적이라 할 수 있다.

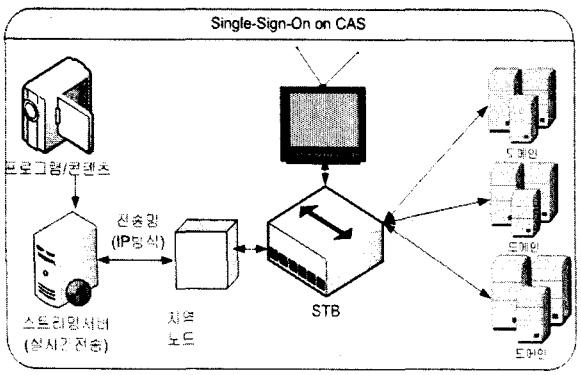


그림 6 SSO on CAS

SSO 접근 방식에서도 중앙저장소 방식의 접근은 빈번한 사용자정보의 이동으로 인한 개방형 네트워크에서의 보안이 비교적 취약하며 일관된 보안정책을 제시함으로서 다양한 서비스 환경을 가지고 있는 IPTV의 개발과 확장성 제공에는 적합하지 않고, 메시지첨부방식은 각 도메인들 간의 보안정책에 관계없이 사용자의 정보를 원활하고 안정적으로 관리/제어할 수 있으므로 분산서비스를 지원하는 IPTV에 더욱 적합하다.

메시지첨부방식의 SAML은 사용자정보에 대한 보안성과 다양한 개발환경에 적용할 수 있는 호환성을 가지고 있어서 다양한 어플리케이션에 대한 각각의 제어 방안이 난립하는 것을 통합된 플랫폼으로 전환할 수 있고, 일관된 보안정책의 일괄 적용으로 보안성도 높아지며, 개발자가 Business Logic에만 전념하게 함으로서 기존 및 신규 어플리케이션에 대한 개발자의 개별 보안모듈 코딩 작업의 증가로 인한 비용을 줄일 수 있다.

## 7. 결론 및 향후 연구방안

본 논문에서는 기존의 DTV환경에서의 제한수신시스템과 SSO의 기능을 융합하여 IPTV환경에 적합한 사용자인증 방안을 제시하였다. 제안한 메시지 첨부방식의 SSO 방식은 다양한 서비스 환경을 기반으로 하는 IPTV서비스에는 매우 적합할 것으로 예상되며, 추후 IPTV-STB를 통한 홈 네트워크의 댁내 가전 제어에도 확장성을 가질 것으로 보인다. 하지만, 중앙저장소 방식과는 달리 IPTV 서비스를 제공하는 각 도메인간의 협의가 있어야 가능한 방식이고 중앙저장소 방식과 비교하여 개방형 네트워크에서 사용자인증정보의 노출이 적기는 하지만 위험도는 존재하는 만큼, 더욱 확실한 정보 암호화 방안이 요구된다.

## 참 고 문 헌

[1] Jeong, J., Shin, D., Shin, D, An XML-based single sign-on scheme supporting mobile and home network service environments, IEEE Transactions on Consumer Electronics 50 (4), pp. 1081-1086, 2004

[2] 조현숙, 이상호, 제한수신시스템을 위한 키 관리 메커니즘과 성능향상 방안, 충북대학교, 2001.2

[3] 임웅택, 김유원, 전문석, 소규모 방송망에 적합한 사설 제한수신 프로토콜의 제안, 전자공학회논문지 제41권 2호, 2004.9

[4] 이장원, 조현숙, 디지털위성방송 제한 수신을 위한 키 관리 스킴 및 시나리오, 학술발표회 논문집, 제15권 3호, 1996.1

[5] Softforum Co.,Ltd, 홈네트워크에서의 SSO, 2005.5