IPTV의 콘텐츠 보호를 위한 스마트카드 인증시스템

황진욱, 김선재, 오해석
*경원대학교 전자계산학과
e-mail: overhawe@ku.kyungwon.ac.kr

Smartcard Authentication for IPTV Contents Protection

Jin-Wook Hwang, Sun-Jae Kim, Hae-Seok Oh
Dept of Computer Science, Kyungwon University

요 약

IPTV(Internet protocol TV)가 상용화되고 가입자 수가 증가하면서 제공하는 콘텐츠의 양이 많아지고 많은 정보를 얻게 되었다. 이러한 많은 콘텐츠의 저작권을 보호하기 위해 수신제한시스템(Conditinal Access System, CAS)과 DRM(Digital Right Management) 기술이 사용되고 있다. 하지만 나날이 발전하는 개인정보의 유출과 해킹을 통한 불법 다운로드, 복제에서 저작권이 위협을 받고 있다. 따라서 현재 서비스 제공자들은 콘텐츠의 저작권을 보호하기 위한 많은 연구들이 진행되고 있다. 본 논문에서는 IPTV에서의 스마트카드를 이용한 인증체계 시스템을 제시하여 기존의 보안시스템보다 더 강화된 보안을 구축 할 수 있다.

1. 서론

인터넷과 컴퓨터기술의 발달로 네트워크를 통한 멀티미디어 데이터를 쉽게 복사 및 변형을 할 수 있게 되었으며, 이로 인하여 새로운 서비스가 제공된 반면에, 디지털 미디어에 대한 저작권 문제가 크게 대두되었다. IPTV를 통하여 전송되는 콘텐츠의 보호는 필수적인 사항으로 어느 정도의 해킹기술이 있다면 IPTV의 콘텐츠를 빼내어 불법으로 유통할 수 있다. 실제로 북미나 유럽에서 이러한 사고가 종종 일어나고 있다[2].

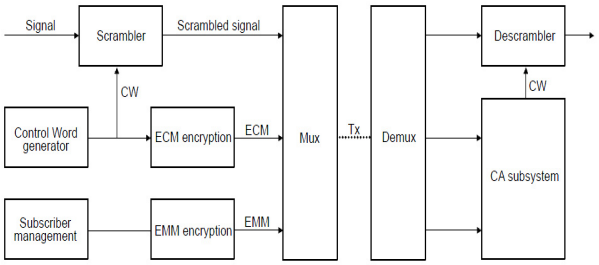
현재 IPTV의 콘텐츠서비스는 보안에 대한 표준이나 모델이 정립되지 않아 여러 가지 다양한 기술이 적용되고 있다. 현재 대표적인 콘텐츠 보안 기술로는 DRM과 수신제한시스템(CAS)이 있다. 하지만 이러한 방식들은 각각 한가지씩만 사용하였을 때 약점을 드러내고 있고, 같이 연동해서 적용 시에는 시스템의 구현이 복잡하고 비용이 많이 드는 단점이 있다. 이러한 콘텐츠를 보호하기 위해 본 논문에서는 스마트카드를 이용한 인증으로 IPTV의 다운로드 서비스에 접근하는 기법을 제안한다.

2. 관련연구

채널관리 IPTV는 사용자가 원하는 콘텐츠를 원하는 시간에 원하는 프로그램을 시청할 수 있는 사용자 맞춤형 시스템이다. 그러나 콘텐츠 보안, 사용자 인증, 콘텐츠 재배포, 과금 등에 문제점을 가지고 있다. 서버의 콘텐츠는 방화벽 등에 의해서 어느 정도 보안이 이루어 질 수 있지만, 아이디/비밀번호 노출시 개인정보의 노출 및 불법사용에 악용의 소지가 있고, 셋탑박스내의 콘텐츠는 불법유통과 같은 문제점이 노출된다, 따라서 이러한 문제를 해결하게 위해 콘텐츠 보안 기술이 필요하다.

2.1 CAS(Conditional Access System)

CAS는 (그림1)에서보는 바와 같이 방송시스템에 가입자(subscriber) 개념을 도입하여 수신자격(entitlement)이 있는 시청자만 특정프로그램을 수신 할 수 있도록 하는 시스템으로 송신기에서 암호화 된 신호를 전송하면 수신 측에서는 비밀키를 이용하여 해독하고 이 과정을 통해 수신인가를 받은 가입자만이 프로그램을 시청 할 수 있도록 한다.



(그림 1) CAS 시스템 구성도

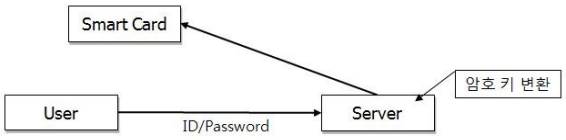
수신자격이 없는 수신자는 시청이 불가능하도록 데이터를 암호화한다. 암호화 된 방송 콘텐츠의 제어는CW(Control Word)를 이용하여 암호화 및 복호화를 처리한다[3].

2.2 스마트카드(Smart Card)

인증은 사용자를 식별하여 사용이 허가 된 사람에게만 콘텐츠를 제공하는 가장 기초적인 보안방법이다. 사용자를 식별하는 방법으로는 간단하게는 ID와 비밀번호를 입력하여 인증하는 방법이 있으며 고급 기술로는 생체인식과 스마트카드 등의 인증을 통하여 식별하는 방법이 있다. 스마트카드는 IC기억소자를 장착하여 대용량의 정보를 담을 수 있는 전자 카드로써 휴대하기 편하고 사용이 간편한 장점이 있다. 실제로 금융, 의료보험, 신용카드 등에 많이 쓰이고 있으며, 대중화된 예를 보면 교통카드로 편리하게 버스나 지하철의 요금을 지불하는 것을 볼 수 있다[1].

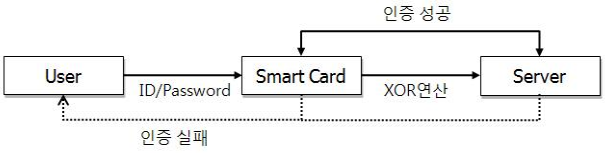
3. 제안하는 시스템

(그림 2)에서는 사용자가 최초 스마트카드를 등록하는 절차를 나타낸 것이다. 먼저 사용자가 스마트카드를 등록하기 위해 자신에 대한 정보(이름, 주민등록번호 등)와 ID, Password를 입력하고 서버로 전송한다. 서버에서는 사용자가 보낸 정보를 바탕으로 속성을 확인하고 비밀 키를 이용하여 암호 키 변환시킨 후에 ID와 함께 저장한다. 그 후 스마트카드에 저장하고 발급받아 등록을 마친다.



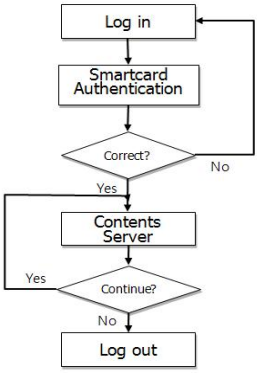
(그림 2) 스마트카드 등록

(그림 3)에서는 스마트카드를 이용한 로그인과 인증에 대해 나타낸다. 먼저 사용자가 등록한 ID와 Password를 입력하면 스마트카드는 이 정보를 받아서 권한이 있는 사용자인지 확인한다. 로그인 정보가 일치하면 스마트카드는 로그인 요청을 받아들여 서버로 전송하고 불일치하다면 거절하여 다시 로그인을 하도록 요청한다. 다음 단계로 서버에서는 스마트카드에서 받은 메시지를 XOR연산을 사용하여 일치한다면 스마트카드와 인증에 성공하게 되고 불일치한다면 로그인 요청을 거절하게 된다.



(그림 3) 스마트카드 로그인 및 인증

(그림 4)에서는 발급받은 스마트카드를 이용하여 IPTV의 콘텐츠를 이용하는 순서도이다. 로그인절차를 마치고 스마트카드의 인증을 통하여 콘텐츠의 서버에 접근이 허가되면 사용자는 서버내의 콘텐츠를 이용할 수 있다. 콘텐츠를 이용하는 동안에는 접속이 유지되며, 콘텐츠를 이용한 후 사용자는 접속을 해제하여 콘텐츠 이용을 종료하게 된다.



(그림 4) 스마트카드 인증을 통한 콘텐츠이용

4. 결론 및 향후연구

본 연구에서는 기존의 시스템보다 보안을 한층 더 강화할 수 있는 스마트카드를 이용한 인증방법을 제시하였다. 스마트카드를 이용하여 인증을 한다면 ID와 Password의 유출이 발생하거나 해킹에 의한 콘텐츠의 불법 다운로드가 발생하더라도 스마트카드의 인증 없이 서버에 접근할 수 없기 때문에 이를 방지 할 수 있다. 향후의 연구방향으로는 스마트카드와 인공지능을 융합하여 서비스업체가 각각의 사용자들에게 공통된 서비스가 아닌 차별화 된 서비스를 제공하여 사용자의 만족도를 높이는 한편, IPTV가 기존의 전파수신방식을 대체하고 보편화 될 수 있다.

Acknowledgments

이 연구는 2009년도 경원대학교 지원에 의한 결과임

참고문헌

[1] 김현석, 김주배, 정연오, 한근희, 최진영 "스마트카드를 이용한 패스워드 기반 인증시스템 정형 분석" 정보과학회 논문지, 시스템 및 이론, 제36권, 제4호, pp.304-310, 2009(8)

[2] 유길상, 트리스탄 바사, 조옥희, 이원형 "CAS를 이용한 IPTV 콘텐츠의 저작권 보호 기법" 한국인터넷정보학회 논문집, 제9권, 제1호, 2008(5)

[3] 윤기송 "CAS-DRM 연동기술" TTA Journel No.117, pp.119-127