경량화된 IPTV 사용자 인증 및 키 동의 프로토콜1)

강용구*, 오희국*
*한양대학교 컴퓨터공학과
kyg@infosec.hanyang.ac.kr, hkoh@hanyang.ac.kr

Lightweight User Authentication and Key Agreement Protocol in IPTV

Yong-Goo Kang*, Hee-Kuck Oh*
*Dept of Computer Science and Engineering, Han-Yang University

요 약

IPTV 시스템에서 서비스 제공자는 제한수신시스템(CAS, Conditional Access System)을 통해 미디어 콘텐츠의 안전한 전송을 제공한다. Scramble Function의 Pseudo-random sequence 생성 초기화 단계에서 사용하는 CW(Control Word)를 허가된 사용자만 획득하게 함으로써 데이터를 보호한다. 적합한 사용자 측에서는 스마트카드를 통해 획득한 CW를 셋톱박스에 전송하고, 셋톱박스는 CW를 이용해 암호화된 데이터로부터 원본의 미디어 콘텐츠를 획득한다. 이 때, CW가 그대로 셋톱박스에게 전송되기 때문에 비인가된 사용자가 공격을 통해 CW를 획득할 수 있어서 암호화된 전송이 요구된다. 이본 논문에서는 스마트카드와 셋톱박스 사이의 암호화 통신을 위해 기존의 방법보다 경량화된 상호인증 및 키 동의 프로토콜을 제안한다.

1. 서론

현대 네트워크 기술의 발달로 전 세계에 걸쳐 디지털 비디오 방송 시스템이 서비스되고 있다. IP망을 통해 방송이나 동영상 콘텐츠, 정보 등을 TV와 이동 단말에 제공하는 통신/방송 융합 서비스가 IPTV이다. 일반적으로 디지털 비디오 스트림은 공개채널을 통해 전송되고, 서비스 제공자는 인가되지 않은 사용자가 전송되는 데이터를 볼 수 없도록 하기 위해 제한수신시스템(CAS, Conditional Access System)을 도입하였다. CAS는 CW(Control Word)를 통해 미디어 콘텐츠를 스크램블하고 인가된 사용자에게만 CW를 제공하여 콘텐츠를 보호한다[1].

SMS(Subscriber Management System)는 스마트카드(Smart Card)를 발행 시 필요한 정보를 저장한다. 스마트카드가 CW를 복원하여 셋톱박스(STB, Set-top Box)에 전달하고, 셋톱박스는 CW를 이용하여 콘텐츠를 복원한다. 이 때, CW를 그대로 전달하기 때문에 McCormac Hack 공격 등으로 비인가자의 CW 획득이 가능하다. 따라서 암호화 통신이 필요하며, 현재 대부분의 IPTV 방송은 단방향이기 때문에 스마트카드와 셋톱박스 사이의 상호인증이 필요하다.

1) 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2009-0080351).

본 논문에서는 사용자측의 스마트카드와 셋톱박스간의 최소의 정보만을 이용한 경량화된 상호인증 및 키 동의 프로토콜을 제안한다. 2장에서는 관련 연구로 기존에 제안된 방법들에 대해 살펴보고, 3장에서는 경량화된 프로토콜을 제안하고, 4장에서 결론을 맺는다.

2. 관련 연구

공개키를 기반으로는 2004년 Jiang 등[2]과 2007년 Hou 등[3]이 제안하였다. Jiang 등의 방법은 전자서명의 지수연산 때문에 계산적인 측면에서 매우 비효율적이다. Hou 등의 방법은 Jiang 등의 방법을 연산량 측면의 효율성을 높였다. 대칭키 기반으로는 2008년 Lee 등이 제안하였다. 이 방법은 XOR연산과, 스마트카드와 셋톱박스 사이에서 공유하는 해시함수를 사용하는 프로토콜이다[4]. 본 논문에서는 필요한 정보만을 사용하면서 요구사항들을 만족하는 안전하고 경량화된 프로토콜을 제안한다.

3. 제안하는 방법

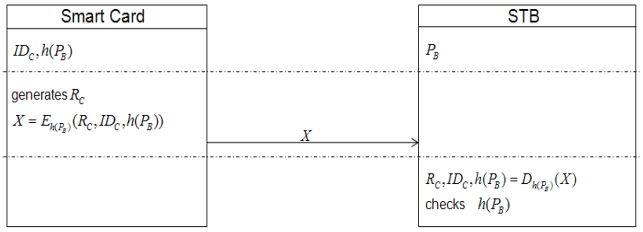
제안하는 방법은 스마트카드와 셋톱박스가 최소한의 정보를 보유하는 상호인증 및 키 동의 프로토콜이다. SMS는 스마트카드 발행 시 프로토콜에 필요한 암호화 알고리즘 및 기본 정보와 함께 스마트카드가 사용될 셋톱박스의 비밀 값을 해시하여 저장한다. SMS는 셋톱박스와의 직접적인 통신은 불가능하고 스마트카드와의 통신 채널과

셋톱박스의 비밀 값은 안전하다고 가정한다. 프로토콜에 사용되는 표기법은 <표 1>과 같으며, 상호인증, 키 동의, 그리고 CW 전송의 총 3단계로 이루어진다.

<표 1> 표기법

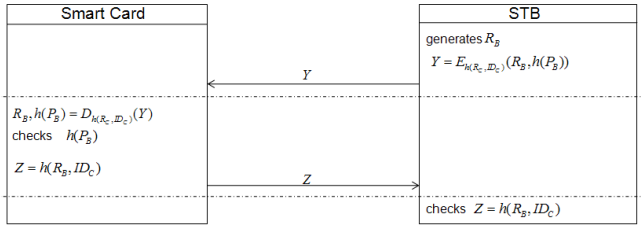
표기법	내용
ID_C	스마트카드의 ID
P_B	셋톱박스의 비밀 값
$h(\cdot)$	단방향 해시 함수
$E_K(\cdot), D_K(\cdot)$	키 K를 이용한 암호화/복호화 연산
R_C, R_B	스마트카드와 셋톱박스가 각각 생성한 랜덤 값
SK	스마트카드와 셋톱박스간의 세션 키

[상호인증] 스마트카드와 셋톱박스간의 상호인증은 먼저 (그림 1)과 같이 시작한다. 셋톱박스는 $h(P_B)$를 통해 X의 무결성을 판단하고 SMS에게 $h(P_B)$를 받은 스마트카드만 X를 생성할 수 있기 때문에 셋톱박스는 스마트카드를 인증한다.



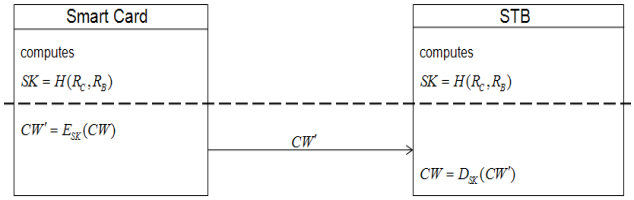
(그림 1) 상호인증 첫 번째 과정

(그림 2)에서 스마트카드는 $h(P_B)$를 통해 Y의 무결성을 판단한다. R_C를 통해 메시지의 최신성을 확인하고 셋톱박스를 인증한다. 셋톱박스는 Z 안의 R_B를 통해 프로토콜의 최신성을 확인한다.



(그림 2) 상호인증 두 번째 과정

[키 동의 및 CW 전송] 상호인증이 수행된 후 스마트카드와 셋톱박스는 (그림 3)과 같이 양측에서 각각 생성한 랜덤값을 이용하여 세션 키를 자체적으로 계산한다. 스마트카드는 생성한 세션 키를 이용하여 CW를 암호화하여 전송하고, 셋톱박스는 CW를 이용하여 원본의 데이터 콘텐츠를 획득한다.



(그림 3) 키 동의 및 CW 전송 과정

4. 결론

본 논문은 사용자측의 스마트카드와 셋톱박스 사이에서 CW의 안전한 전송을 위한 상호인증 및 키 동의 프로토콜을 제안하였다. 프로토콜에 사용되는 각 메시지들은 랜덤 값을 사용하여 최신성을 보장하고, McCormac Hack 공격을 예방할 수 있다. 또한 기존 연구에서 사용하던 불필요한 정보를 없애고 최소의 정보만을 이용하여 프로토콜을 경량화하였다. 발행된 스마트카드가 사용될 셋톱박스 정보를 서비스 제공자로부터 추가로 제공받음으로써 스마트카드의 확장성 있는 사용이 가능하다.

참고문헌

[1] F. Tu, C. Laih, and H. Tung, “On Key Distribution Management for Conditional Access System on Pay-TV System,” IEEE Trans. On Consumer Electronics, Vol. 45, pp.151-158, 1999.

[2] 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, pp.882-886, 2004.

[3] T. Hou, J. Lai and C. Yeh, “Based on Cryptosystem Secure Communication between Set-top Box and Smart card in DTV Broadcasting,” TENCON 2007, IEEE Region 10 Conference, pp.1-5, 2007.

[4] Ji Seon Lee, Hyun Sook Rhee, and Dong Hoon Lee, “Efficient and Secure Communication between Set-top Box and Smart Card in IPTV Broadcasting,” International Conference on Convergence and Hybrid Information Technology, Vol. 00, pp.307-310, 2008.