IPTV환경에서 사용자 인증을 위한 스마트카드 키 동의 프로토콜[1)]

서화정○ 김호원
부산대학교 컴퓨터 공학과
hwajeong@pusan.ac.kr, howonkim@pusan.ac.kr

Smartcard Key Agreement Protocol for User Authentication in IPTV Broadcasting

Hwa-Jeong Seo○ Ho-won Kim
Department of Computer Science Engineering Pusan National University

1. 서 론

IPTV(Internet Protocol television)는 기존의 아날로그 방식의 서비스를 제공하는 대신 인터넷 프로토콜을 통해 대용량의 멀티미디어 데이터를 사용자에게 제공하는 서비스이다. 하지만 디지털 정보를 통해 제공되는 컨텐츠는 쉽게 복제가 가능하여 권한이 없는 사용자들에 의해 불법으로 서비스를 사용하는 것이 가능하다. 이를 방지하기 위해 실시간 방송 서비스와 VOD(Video on Demand)서비스는 접근제한시스템을 통해 권한이 있는 사용자에게만 서비스를 제공하는 유료화 정책을 추진하고 있다. 본 논문에서는 컨텐츠에 대한 접근권한을 가지는 사용자와 서비스 공급업체간에 안전한 인증 프로토콜을 제안한다. 해당 프로토콜은 기존에 제안된 프로토콜에 비해 효율적일뿐 아니라 재전송공격, 스마트카드 복제, MacCormac hack 공격 문제를 해결한다.

2. 제안하는 프로토콜

제안하는 프로토콜은 기존에 제안된 프로토콜의 효율성을 만족시키면서 McCormac Hack 공격과 재전송 공격에도 안전한 프로토콜이다. 세션키는 세션마다 새롭게 생성되는 임의의 난수값을 Diffie-Hellman기법을 통해 생성함으로써 안전한 키 분배가 이루어 진다[1].

■ 등록 단계 SMS는 STB의 비밀값과 스마트카드의 아이디값을 해시연산하여 메시지 C_1을 생성한다. C_1은 해시연산, 마스터키와 함께 스마트카드로 보내지게 된다.

■ 로그인 단계

스마트카드는 난수 R_{SC}를 생성하며 자신의 비밀키값 K_{SC}를 해시하여 C_1과 Xor연산을 통해 $h(K_{STB}\|ID_{SC})$를 계산할수 있다. 해당 값은 타임스탬프와 난수 R_{SC}를 해시연산을 수행하여 C_2를 생성한다. C_3은 난수와 $h(K_{STB}\|ID_{SC})$값을 Xor연산하여 생성한다. 생성원 g에는 난수값을 지수승하여 $g^{R_{SC}}$을 계산한다. 계산된 $C_2, C_3, g^{R_{SC}}$값과 ID_{SC}, T값은 스마트카드에서 STB로 전송된다.

■ 상호인증 단계

STB는 스마트카드로부터 전송받은 타임스탬프를 확인하여 제한된 시간안에 도착한 유효한 값인지 확인한다. 이어서 C_4값을 자신의 비밀키값을 통해 계산한다. C_4값은 전송되어온 C_3값에 Xor연산하여 스마트카드의 난수값 R_{SC}를 계산한다. 그 다음 C_4에 타임스탬프와 R_{SC}를 해시연산하여 C_2와 동일한지 확인하고 유효한 경우 다음단계를 수행한다. STB는 스마트카드와의 상호 인증에 필요한 메시지 C_5과 난수값 R_{STB}를 생성원 g에 지수승연산하여 스마트 카드에게 전송하게 된다. 스마트카드는 $h(h(K_{STB}\|ID_{SC})\|T\|R_{SC}+1)$

1) 이 논문 또는 저서는 2010년 교육과학기술부로부터 지원받아 수행된 연구임" (지역거점연구단육성사업/차세대물류IT기술연구사업단

을 계산하여 C_5와 비교하여 동일한 경우 STB를 인증하게 된다.

■ 키 공유 단계

스마트카드는 전송되어온 $g^{R_{STB}}$에 자신이 가진 난수값 R_{SC}를 지수승 연산하여 세션키를 계산한다. 마찬가지로 STB는 스마트카드로부터 전송받은 $g^{R_{SC}}$에 자신의 난수값 R_{STB}를 지수승하여 세션키를 계산할 수 있다.

■ 제어 단어 전송 단계

세션키를 가진 스마트카드는 STB에게 세션키를 통해 암호화된 제어단어를 전송함으로써 원하는 서비스를 제공받을 수 있다.

3. 효율성 분석

[표 1]는 각 프로토콜의 효율성에 대해 나타낸다. Kim이 제안한 프로토콜은 연산량이 비교적 적은 Xor 연산과 해쉬연산을 사용한다. 따라서 다른 프로토콜에 비해 연산량이 줄어드는 장점이 있다. 하지만 안전성 측면에서 지수 연산과 대칭키 암호화를 사용하는 프로토콜에 비해 취약하다고 할 수 있다. 또한 Lee에 의해 제시된 프로토콜은 많은 대칭키 기반 암호화와 해시연산을 사용하여 연산량이 증가한다. 하지만 본 논문에서 제시하는 프로토콜은 지수연산과 적은 해시연산과 Xor연산을 사용함으로써 대칭키기반의 암호화보다 적은 연산량을 가지고 상호간의 인증이 가능하다.

표 1 프로토콜들의 계산량 비교

프로토콜	계산량				
	등록단계	로그인단계	상호인증단계	키동의단계	총계
제안하는프로토콜	2H+1O	1E+1H+1O	1E+4H+1O	1E	7H+3E+3O
Kim의 프로토콜[2]	2H+1O	2H+3O	5H+11O	1H	10H+15O
Lee의 프로토콜[3]	2H+2S	2H	9H+3S	3H	16H+5S
H:해시함수, E:지수연산, S:대칭키 연산, O:XOR연산					

4. 결론

본 논문에서는 접근제한 시스템이 가지는 스마트카드 복제문제와 McCormac Hack 공격 그리고 재전송 공격과 같은 STB와 스마트카드간에 존재하는 문제점을 해결하였다. 또한 지금까지 제안된 다른 프로토콜과 비교해 보다 효율적인 연산을 통해 안전성을 제공하는 프로토콜을 제안하였다. 따라서 IPTV환경에서 사용자는 스마트카드를 사용하여 안전하게 서비스이용이 가능하며 사용자 인증에 따른 시간지연 문제도 줄어 들것이다.

참고 문헌

[1] W.Diffe and M. Hellman "New Direction in Cryptography," IEEE Transaction on Information Theory, vol. 22, no. 6, pp. 664-654, Nov. 1976.

[2] H. Kim, "Secure communication in digital TV broadcasting," International Journal of Computer Science and Network Security (IJCSNS), vol. 8, no. 9, pp. 1-5, Sep. 2008.

[3] 이훈정, 손정갑, 오희국, "IPTV환경에서 스마트카드와 셋톱박스간의 안전한 통신을 위한 경량화된 키 동의 프로토콜," 정보보호학회논문지, vol. 20, no. 3, pp. 67-78, Jun, 2010.