情報保護學會論文誌
第20卷 第3號, 2010. 6

IPTV환경에서 스마트카드와 셋톱박스간의 안전한 통신을 위한 경량화된 키 동의 프로토콜*

이 훈 정,† 손 정 갑, 오 희 국‡
한양대학교 컴퓨터공학과

A Lightweight Key Agreement Protocol between Smartcard and Set-Top Box for Secure Communication in IPTV Broadcasting*

Hoonjung Lee,† Junggab Son, Heekuck Oh‡
Department of Computer Science and Engineering, Hanyang University

요 약

IPTV환경의 유료 TV시스템에서는 권한이 없는 사용자의 프로그램 시청을 막기 위한 방법으로 접근제한시스템을 사용한다. 접근제한시스템에서 스마트카드는 스크램블된 프로그램을 디스크램블하는 과정에서 필요한 제어 단어를 셋톱박스에 전달하는 역할을 한다. 제어 단어에 대한 해킹은 유료 TV시스템에서 심각한 보안이슈 중 하나이다. 제어 단어의 안전한 전송을 위한 스마트카드와 셋톱박스간의 안전한 통신채널 생성에 관한 많은 연구가 진행되었으나 기존에 제안된 방법들에선 효율성과 안전성측면에서 문제점들이 발견되었다. 본 논문에서는 대칭키 기반 알고리즘을 사용한 경량화된 키 동의 프로토콜을 제안한다. 기존에 제안된 프로토콜들과의 연산량 비교를 통해 다른 프로토콜들에 비해 효율적임을 보이고 제안하는 프로토콜의 보안 요구사항에 대한 안전성 분석을 하였다.

ABSTRACT

CAS(Conditional Access System) is used in Pay-TV System to prohibit unauthorized user(s) accessing the contents in IPTV broadcasting environment. In the CAS, Smartcard transfers CW which is necessary in the process of descrambling the scrambled program to STB. CW hacking problem is one of the most serious problems in pay-TV system. There have been many researches on generating secure communication channel between smartcard and STB for secure transmitting, But they had problems in efficiency and security. In this paper, we propose a lightweight key agreement protocol based on a symmetric key algorithm. We show that our proposed protocol is more efficient than existing protocols by comparing the amount of computations, and analyzing the security requirement of the proposed protocol.

Keywords: IPTV, CAS, Key Management

접수일(2009년 11월 17일), 수정일(1차: 2010년 2월 25일, 2차: 2010년 3월 25일), 게재확정일(2010년 3월 25일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (NIPA-2010-C1090-1011-0010)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임. (No. 2010-0000438)
† 주저자, hjlee@infosec.hanyang.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr

I. 서 론

최근 몇 년간 유무선 네트워크의 전송속도의 급격한 발전으로 네트워크를 이용해 방송 콘텐츠와 같은 대용량 멀티미디어 데이터를 전송할 수 있게 되었으며 이러한 기술의 발달로 IP 방식의 인터넷망을 이용해 방송 콘텐츠제공이 가능한 IPTV 서비스가 가능하게 되었다. IPTV환경은 아날로그 환경이 아닌 디지털 환경이다. 디지털 환경에서는 콘텐츠를 복사하여도 원본의 품질과 동일한 복사본을 만들 수 있다. 인터넷을 통한 콘텐츠의 유통은 무료라는 생각에 현재까지도 P2P나 웹하드등을 통해 고품질의 디지털 콘텐츠들이 널리 퍼져 있어 콘텐츠 제작자나 제공자들이 많은 손해를 입고 있다. 이에 IPTV서비스는 기존의 디지털 위성, 지상파, 케이블 방송과 같은 실시간 방송 서비스와 사용자가 원하는 방송을 골라서 볼 수 있는 VoD(Video on Demand)서비스 모두에 유료화 정책이 추진되고 있다.

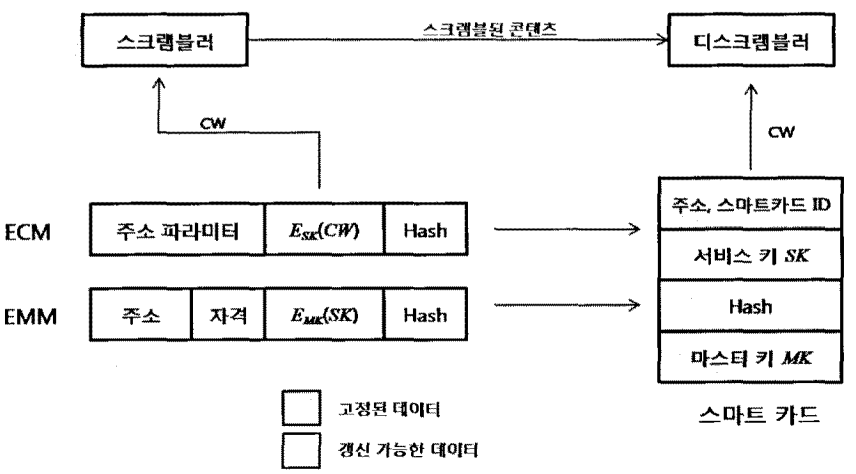
기존의 위성, 지상파, 케이블 방송시스템에서는 유료 콘텐츠에 대한 권한이 없는 사용자들의 불법시청을 막기 위해 접근제한시스템을 사용하고 있으며, PC와 인터넷 환경에서는 콘텐츠 보호를 위해 다양한 DRM(Digital Right Management)기술들이 사용되고 있다. IPTV환경에서도 기존의 방식들을 그대로 적용해 실시간 방송 서비스 콘텐츠 보호에는 접근제한시스템을, VoD 서비스 콘텐츠의 보호에는 DRM을 사용하고 있다.

이 논문에서는 콘텐츠 보호 기술중 실시간 방송 콘텐츠 보호에 사용되는 기술인 접근제한시스템에서 제어 단어 해킹 문제인 McCormac Hack문제와 스마트카드 복제 문제에 대해 소개한 후 이를 방어할 수 있는 방법에 대해서 다룬다. 이어지는 논문의 구성은 다음과 같다. 2장에서는 접근제한시스템에 대한 내용과 접근제한시스템이 가지는 문제점에 대해 설명하고, 3장에서 기존에 제안된 방법들에 대해 알아본 후, 4장에서 이 논문에서 제안하는 방법에 대해 자세히 기술한다. 5장에서는 기존의 방법들과 제안하는 방법을 비교분석 하고, 6장에서는 결론과 향후 연구방향을 제시한다.

II. 연구배경

2.1 접근제한시스템 (Conditional Access System, CAS)

접근제한시스템은 사용자의 조건에 따라 접근을 제한하는 시스템으로 유료 TV 시스템에서 인가된 사용자만이 해당 프로그램에 접근할 수 있도록 하는 콘텐츠 보안 솔루션이다[1]. 접근제한시스템은 크게 두 가지 기능을 수행한다. 첫째는 CSA(Common Scrambling Algorithms)[2]라는 스크램블링 알고리즘을 사용하여 콘텐츠를 스크램블링/디스크램블링 하는 기능이고, 두 번째는 스크램블링/디스크램블링에 필요한 여러 키들을 계층적으로 관리하는 기능이다. 그림 1은 접근제한시스템의 구성도이다. 방송을 전송하는 쪽에서 제어 단어(Control Word, CW)를 생성하고 생성된 제어 단어를 이용해 방송 콘텐츠를 스크램블링하여 전송한다. 이때 생성된 제어 단어는 서



〔그림 1〕 접근제한시스템 구성도

비스 키(Service Key, SK)로 암호화되어 자격제어메시지(Entitlement Control Message, ECM)을 통해 전송되고, 서비스 키는 각 사용자의 스마트카드에 저장되어 있는 마스터 키(Master Key, MK)로 암호화 되어 자격관리메시지(Entitlement Management Message, EMM)을 통해 전송된다. 수신측에는 송신측과 반대의 과정을 수행하게 되는데 자격관리메시지를 통해 전송되는 마스터 키로 암호화된 서비스 키를 복호화하여 자신의 스마트카드에 저장되어 있는 서비스 키를 갱신하고, 자격제어메시지를 통하여 전송되는 서비스 키로 암호화 된 제어 단어를 복호화한 후, 제어 단어를 이용해 콘텐츠를 디스크램블링하여 시청 할 수 있게 된다.

2.2 현재 접근제한시스템의 문제점

현재 위성, 지상파, 케이블 방송시스템에서 널리 사용되고 있는 접근제한시스템은 하나의 스마트카드로 같은 접근제한시스템을 사용하는 서로 다른 셋톱박스(Set-Top BOX, STB)에서 사용이 가능하다. 2001년 Kanjanarin등은 접근제한시스템의 이러한 특성 때문에 생겨난 스마트카드 복제 문제와 McCormac Hack 공격에 대해 이야기 하였다[3].

스마트카드 복제 문제는 권한이 있는 사용자의 스마트카드를 복제하여 권한이 없는 사용자들이 같은 종류의 STB에서 인가된 사용자처럼 사용하는 문제이고, McCormac Hack 공격은 STB와 스마트카드 간의 통신 채널을 공격하여 제어 단어를 얻어낸 후, 그것을 불법적으로 사용하는 문제이다. 방송 수신단인 STB에서는 자격관리메시지와 자격제어메시지를 이용해 제어 단어를 얻는 모든 과정이 사용자의 스마트카드에서 이루어진다. 스마트카드가 제어 단어를 얻은 후, 스크램블링된 콘텐츠의 디스크램블링을 위해 이 제어 단어를 STB의 디스크램블러에 전달해 주게 되는데, 이 전달 과정에서 스마트카드와 STB간의 통신 채널을 도청하여 제어 단어를 획득하는 것이 가능하다. 공격자에 의해 획득된 제어 단어를 STB의 디스크램블러에 직접 입력하면 유료 방송 콘텐츠에 불법적으로 접근하는 것이 가능하다.

스마트카드복제와 McCormac Hack 공격 등으로 비인가된 사용자의 불법적인 방송시청이 가능할 경우 이는 방송 사업자들의 이익과 직결되는 커다란 문제가 된다. 최근에 방송 사업자들은 이러한 문제를 해결하기 위해 Irdeto와 Conax에서 제공하는 STB에 보안칩을 내장하는 방식을 도입하였다[4],[5]. 이 방식에서 STB에 내장된 보안칩은 스마트카드와 STB사이에 보안 채널을 형성하는데 사용된다. 즉, 스마트카드는 암호화된 제어 단어를 STB로 전송하고, STB는 내장된 보안칩을 사용해 암호화된 제어 단어를 복호화하여 STB의 디스크램블러에게 전달하게 된다. 이러한 방식은 자격제어메시지를 통해 전달되는 제어 단어가 STB에 내장되어 있는 보안칩에 저장되어 있는 키로 암호화되어 있어야 한다. 보안칩과 같은 하드웨어 기반의 접근제한시스템은 생산 및 갱신에 많은 비용이 들어간다. 특히 갱신이 필요할 경우 STB에 내장되어 있는 칩 자체를 교체해야 하기 때문에 갱신이 거의 불가능하다고 할 수 있다.

III. 관련 연구

현재까지 보안칩과 같은 하드웨어를 사용하지 않는 환경에서 스마트카드 복제 문제와 McCormac Hack 공격에 관한 많은 연구가 진행 되었다. 그러나 기존에 제안된 프로토콜들은 연산의 효율성이나 프로토콜의 안전성 측면에서 문제점들이 지적되었다.

2004년 Jiang 등은 Schnorr의 디지털서명 기법과 일방향 해쉬함수를 사용하는 스마트카드와 STB간의 키 교환 프로토콜을 제안하였다[6]. 2006년 Yoon 등[7][8]은 Jiang 등의 프로토콜이 키 교환 프로토콜의 보안 요구사항 중 위장공격(Impersonation attack)과 완전한 전방향 안전성(Perfect forward secrecy)을 만족하지 못함을 보이고 새로운 키 교환 프로토콜을 제안하였다. 2007년 Hou 등은 Jiang 등이 제안한 프로토콜보다 연산량 측면에서 보다 효율적인 키 교환 프로토콜을 제안하였다[9]. 2008년 Kim[10]은 Hou 등이 제안한 키 교환 프로토콜이 공격자의 메시지 변조에 따른 위장공격에 취약함을 보이고, 이를 보완함과 동시에 지수연산을 이용하지 않는

〔표 1〕 Kim과 Lee 등의 프로토콜에서 사용하는 표기법

표기법	내용
ID_C	스마트카드의 ID
ID_S	STB의 ID
x_S	STB의 비밀키
PW	사용자의 비밀번호
$h(\cdot)$	일방향 해쉬함수
$E_K(\cdot)/D_K(\cdot)$	키 K를 이용한 대칭키 암호화/복호화

연산량을 줄인 키 교환 프로토콜을 제안하였으며, 2009년 Lee등은 Yoon 등이 제안한 프로토콜이 위장공격이 가능함을 보이고 이를 개선한 프로토콜을 제안하였다[11].

Kim이 제안한 키 교환 프로토콜은 Jiang, Hou 등의 프로토콜에서 지적 되었던 위장공격 및 제어 단어가 노출되는 McCornmac Hack 공격에 취약하다. Yoon 등은 세션키를 알아내 위장공격이 가능하다고 했으나 세션키를 알아낸다는 것은 제어 단어가 노출되는 것과 같은 의미이므로 위장공격보다 더 근본적인 McCormac Hack 공격이 가능하다고 할 수 있다. 또한, Lee등이 제안한 키 교환 프로토콜은 수학적 가정에서 완전하지 않으며, 연산량 측면에서도 기존의 프로토콜에 비해 비효율적이다. 이 장에서는 Kim이 제안한 프로토콜과 Lee 등이 제안한 프로토콜에 대한 분석을 통해 각각의 프로토콜이 가지는 문제점에 대해 분석한다. 표 1은 Kim과 Lee 등이 제안한 프로토콜 기술에 사용된 표기법이다.

3.1 Kim이 제안한 프로토콜에 대한 분석

Kim이 제안한 프로토콜에서 스마트카드와 STB는 각각의 비밀값인 사용자의 비밀번호와 STB의 비밀키는 알 수 없지만 XOR연산의 특성을 이용해 그 비밀정보가 포함된 어떠한 비밀값을 계산할 수 있음을 보임으로써 상대방을 인증하는 방식을 사용한다. Kim의 프로토콜은 등록단계, 로그인 단계, 상호인증 단계, 키 공유 단계, 제어 단어 전송단계의 5단계에 걸쳐 프로토콜을 진행된다.

■등록단계

SMS(Subscriber Management System)는 $IP=h(ID_C,PW)$, $C=IP\oplus h(ID_C,x_S)$, ID_S, $h(\cdot)$, 스마트카드의 마스터 비밀키(MPK)를 스마트카드에 저장하여 사용자에게 전달한다.

■로그인 단계

스마트카드는 STB에게 $CID_c=ID_C\oplus h(ID_S)$, $C_2=h(T\oplus C\oplus IP)$, 임의의 변수 r, 타임스탬프 T를 전송한다.

■상호인증 단계

STB는 $C_2'=h(T\oplus h(ID_C,x_S))$를 계산한 후, 다음과 같은 수식을 통해 C_2와 C_2'이 같은지를 검증한다.

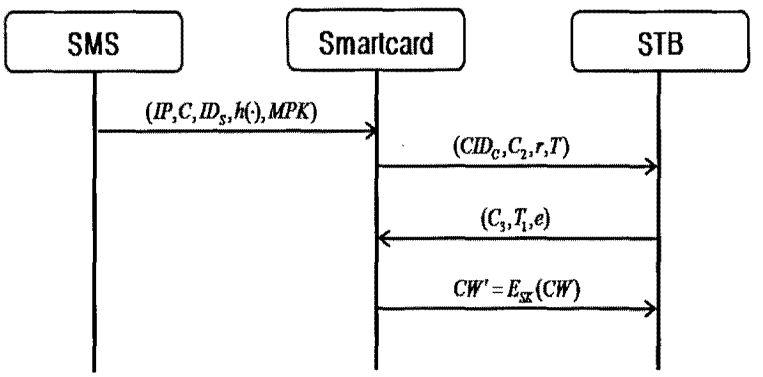
$$\begin{aligned}C_2&=h(T\oplus C\oplus IP)\\&=h(T\oplus IP\oplus h(ID_C,x_S)\oplus IP)\\&=h(T\oplus h(ID_C,x_S))\\&=C_2'\end{aligned}$$

두 값이 같을 경우 임의의 변수 e, 타임스탬프 T_1, $C_3=h(C_2'\oplus ID_S\oplus T_1\oplus e')$를 스마트카드에 전송한다. 이때 C_3 생성에 필요한 e'는 STB의 ID ID_S의 해쉬값, 변수 e, 스마트카드가 생성한 타임스탬프 T를 XOR한 값으로 e를 알고 있는 사용자만이 생성할 수 있는 값이다.

$$e'=h(ID_S)\oplus e\oplus T$$

스마트카드는 $C_3'=h(C_2\oplus ID_S\oplus T_1\oplus e')$를 계산한 후, 다음과 같은 수식을 통해 C_3와 C_3'가 같은지를 검증한다.

$$\begin{aligned}C_3&=h(C_2'\oplus ID_S\oplus T_1\oplus(h(ID_S)\oplus e\oplus T))\\&=h(C_2\oplus ID_S\oplus T_1\oplus(h(ID_S)\oplus e\oplus T))\\&=C_3'\end{aligned}$$



〔그림 2〕 Kim의 프로토콜

■키 동의 단계

상호인증을 마친 후 스마트카드와 STB는 각각 세션키 $SK=h(r,e,ID_C,ID_S)$를 생성하여 공유하게 된다.

■제어 단어 전송 단계

스마트카드는 키 동의 단계에서 공유한 SK를 이용해 암호화된 $CW'=E_{SK}(CW)$를 STB에 전송하고, STB는 공유된 SK를 이용해 $CW=D_{SK}(CW')$를 복호화하여 CW를 얻을 수 있다.

Kim이 제안한 프로토콜은 Jiang, Hou 등이 제안한 프로토콜들과 같이 위장공격에 취약하다. STB의 ID는 강력한 비밀을 요구하는 값이 아니므로 공격자는 stolen-verifier 공격[12]이나 서버 데이터 도청[13]등 다양한 공격방법을 통해 STB의 ID를 얻는 것이 가능하다. STB의 ID ID_s를 얻으면 CID_C와의 XOR연산을 통해 스마트카드의 ID ID_C도 쉽게 얻을 수 있다. r과 e는 보안되지 않는 네트워크를 통해 전송되는 값이므로 이 값들 역시도 쉽게 얻을 수 있다. 공격자는 세션키 생성에 필요한 모든 값을 얻어 세션키를 생성 할 수 있으며, 생성한 세션키를 이용해 제어 단어를 얻어 낼 수 있으므로 McCormac Hack 공격이 가능하다.

3.2 Lee 등이 제안한 프로토콜에 대한 분석

Lee 등이 제안한 프로토콜에서는 Diffie- Hellman 키 동의 기법[14]을 이용하고 있다. Lee 등의 프로토콜에서는 체에서의 나눗셈 연산을 통해 상대방을 인증하는 방식을 사용한다. Lee 등의 프로토콜은 Kim이 제안한 프로토콜과 마찬가지로 등록단계, 로그인 단계, 상호인증 단계, 키 공유 단계, 제어 단어 전송단계의 5단계에 걸쳐 진행된다.

■등록단계

SMS는 $R=h(ID_C\oplus x_S)\oplus h(PW)$, g, ID_S, $h(\cdot)$, 스마트카드의 마스터 비밀키(MPK)를 스마트카드에 저장하여 사용자에게 전달한다. 여기서 p와 q는 서로 다른 큰 소수이며 q는 $p-1$의 소인수이다. g는 $GF(p)$의 원시원소이다.

■로그인 단계

스마트카드는 다음과 같은 값들을 계산한 후, STB에게 ID_C와 Y를 전송한다.

$A=g^a \bmod p$와 $X=R\oplus h(PW)=h(ID_C\oplus x_S)$값을 이용해 $Y=h(X,ID_C,ID_S)\cdot A$를 계산한다. 여기서 a는 Z_q^*의 임의의 원소이다.

■상호인증 단계

STB는 다음과 같은 값들을 계산한 후, 스마트카드에게 B와 M을 전송한다.

$B=g^b \bmod p$, $M=h(K,X,B,ID_C,ID_S)$. 여기서 b는 Z_q^*의 임의의 원소이다. K는 아래와 같이 계산할 수 있다.

$$K=\left(\frac{Y}{h(h(ID_C\oplus x_S),ID_C,ID_S)}\right)^b$$
$$=\left(\frac{h(h(ID_C\oplus x_S),ID_C,ID_S)\cdot A}{h(h(ID_C\oplus x_S),ID_C,ID_S)}\right)^b$$
$$=A^b=g^{ab}$$

스마트카드는 $K=B^a=g^{ab} \bmod p$와 $M=h(K,X,B,$

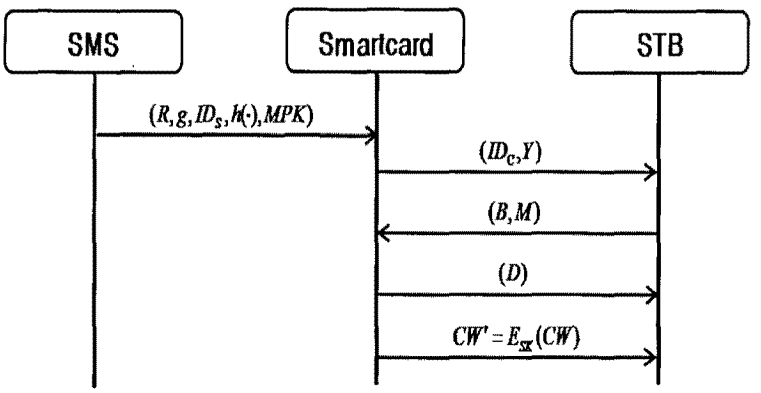


그림 3. Lee 등의 프로토콜

ID_C, ID_S)를 계산해서 M과 M'이 같은지를 검증한다.

■키 동의 단계

스마트카드는 $D=h(K,A,B,ID_C,ID_S)$를 계산해 STB에게 전송하고 STB는 $D'=h(K,A,B,ID_C,ID_S)$을 계산해 D'과 D가 동일한지 검증한 후, D값을 공유키로 사용한다.

■제어 단어 전송 단계

스마트카드는 키 동의 단계에서 공유한 SK를 이용해 암호화된 $CW'=E_{SK}(CW)$를 STB에 전송하고, STB는 공유된 SK를 이용해 $CW=D_{SK}(CW')$를 복호화하여 CW를 얻을 수 있다.

Lee 등이 제안한 프로토콜은 Yoon 등이 제안한 프로토콜이 가지는 문제점인 위장공격을 해결하고자 제안한 논문이다. 그러나 Lee 등의 논문에서 사용된 함수들은 Yoon 등의 프로토콜에서 정의해놓은 표기법과 함수들을 그대로 사용하는데 Lee 등의 프로토콜에서 사용하는 암호학적 해쉬함수는 Yoon 등이 정의한 일반적인 암호학적 해쉬함수와는 다른, 결과값을 Z_q^*의 원소로 사상해주는 암호학적 해쉬함수를 사용해야만 프로토콜이 정상적으로 동작한다. 또한 Lee 등의 프로토콜은 체에서의 나눗셈 연산을 통해 상대방을 인증하고 있는데 실제로 체에서의 나눗셈은 역원을 곱하는 연산이다. 이는 기존에 제안된 프로토콜들에 비해 역원을 구하는 연산이 추가로 발생하게 되므로 연산량 측면에서 비효율적인 프로토콜이라 할 수 있다.

3.3 기존 연구들에 대한 고찰

현재까지 제안된 프로토콜들의 수행 환경은 다음과 같다. SMS은 가입자의 스마트카드와 STB의 ID와 비밀키 등 가입자 관련 정보를 저장하고 관리한다. 방송가입자는 SMS로부터 ID, 비밀키와 같은 자신의 가입정보가 조작 불가능한 저장장치에 저장되어 있는

표 2. 제안하는 프로토콜에서 사용하는 표기법

표기법	내용
ID_{SC}	스마트카드의 ID
ID_{STB}	STB의 ID
K_{SC}	스마트카드의 비밀키
K_{STB}	STB의 비밀키
$h(\cdot)$	일방향 해쉬함수
$E_K(\cdot)/D_K(\cdot)$	키 K를 이용한 대칭키 암호화/복호화
R_{SC}/ R_{STB}	스마트카드, STB가 각각 선택하는 임의의 난수

스마트카드를 발급받게 된다. 또한 사용자의 STB에는 STB의 비밀키가 STB내 시큐어 플래쉬와 같은 조작 불가능한 비휘발성 저장 장치에 저장되어 있다. STB는 자격관리메시지, 자격제어메시지 등의 방송신호로부터는 어떠한 정보도 얻을 수 없고, 스마트카드가 전달해 주는 정보만을 이용할 수 있다. 스마트카드와의 인증 시에도 SMS가 스마트카드를 통해서 전달하는 값만을 사용한다.

기존에 제안된 대부분의 프로토콜들은 공개키 암호시스템이나 Diffie-Hellman 키 동의 프로토콜을 사용하였다. 공개키 암호시스템 사용의 경우 공개키의 인증을 위한 인증서의 검증 및 철회등 공개키 기반구조 관리에 관한 문제가 있고, Diffie-Hellman 키 동의 프로토콜 사용의 경우 잘 알려진 약점인 인증기능이 없어 중간자 공격에 취약하다는 문제를 해결해야 한다. 기존 연구들에서는 Diffie-Hellman 키 동의 프로토콜의 이러한 약점의 극복을 위해 XOR연산과 체상에서의 역원 연산을 이용해 인증기능을 추가하고자 하였다. 그러나 지수 연산에 따른 연산량의 증가와 XOR연산에 따른 프로토콜의 안전성 약화를 가져왔다.

IPTV 또는 디지털 방송 환경에 존재하는 서비스 제공자의 SMS는 스마트카드와 STB에 대한 비밀정보를 알고 있다. 방송환경의 이러한 점을 이용하면 기존의 연구들처럼 공개키 암호시스템이나 Diffie-Hel-

표 3. SMS에 저장되어 있는 스마트카드-STB쌍의 ID와 비밀키 정보

번호	스마트카드 ID	스마트카드 비밀키	STB ID	STB 비밀키
1	ID_{SC_1}	K_{SC_1}	ID_{STB_1}	K_{STB_1}
2	ID_{SC_2}	K_{SC_2}	ID_{STB_2}	K_{STB_2}
⋮	⋮	⋮	⋮	⋮
n	ID_{SC_n}	K_{SC_n}	ID_{STB_n}	K_{STB_n}

Iman 키 동의 프로토콜을 사용하지 않고도 인증이 가능하다. 다음장에서는 이 논문에서 제안하고 있는 대칭키 암호시스템과 시도-응답 방식을 이용한 인증과 키 동의 방법에 대해 다룰 것이다.

IV. 제안하는 프로토콜

제안하는 프로토콜은 SMS가 스마트카드와 STB의 ID와 비밀키를 사전에 공유하고 있는 환경에서 대칭키 암호기법과 시도-응답 방식을 이용한 인증된 키 동의 프로토콜이다. 즉, SMS는 스마트카드에게는 STB와의 인증에 필요한 정보를 스마트카드의 비밀키로 암호화하여 전달하고, STB에게는 스마트카드와의 인증에 필요한 정보를 STB의 비밀키로 암호화하여 스마트카드를 통해 전달받게 하였다. 키를 알고 있는 개체만이 인증에 필요한 정보를 복호화 할 수 있기 때문에 복호화한 값을 이용한 시도-응답 방식을 통해 상대방을 인증한 후, 임의의 난수값을 이용해 세션키를 생성하는 방식의 프로토콜이다.

제안하는 프로토콜은 등록단계, 로그인 단계, 상호인증 단계, 키 공유 단계, 제어 단어 전송단계의 5단계에 걸쳐 프로토콜을 진행한다. 표 2는 이 논문에서 제안하는 프로토콜 기술에 사용하는 표기법이다.

■ 등록단계

SMS는 표 3과 같이 서버에 스마트카드와 그에 대응되는 STB의 ID와 비밀키를 저장하여 관리한다.

SMS는 서버에 저장되어 있는 스마트카드와 STB 쌍의 정보로 $PI = E_{K_{SC}}(PI_{STB}) \| E_{K_{STB}}(PI_{SC})$ 값을 생성하여 $h(\cdot)$, 스마트카드의 마스터 비밀키(MPK)와 함께 스마트카드에 저장하여 사용자에게 전달한다. PI값 계산에 필요한 PI_{STB}와 PI_{SC}는 다음과 같다.

$$PI_{STB} = h(K_{STB} \| ID_{SC}),\ PI_{SC} = h(K_{SC} \| ID_{STB})$$

■ 로그인 단계

스마트카드는 STB에게 SMS로부터 수신한 정보 중 STB의 비밀키로 암호화 되어있는 $E_{K_{STB}}(PI_{SC})$와 $C_1 = h(PI_{SC} \| h(PI_{STB} \| R_{SC}))$, ID_{SC} 그리고 임의의 난수 R_{SC}를 전송한다.

■ 상호인증 단계

C_1을 수신한 STB는 C_1'를 계산하여 C_1과 C_1'이 같음을 검증한 후, 값이 동일할 경우, $C_2 = h(PI_{STB} \| h(PI_{SC} \| R_{STB}))$, ID_{STB} 그리고 임의의 난수 R_{STB}를 전송한다.

STB는 자신의 비밀키 K_{STB}와 스마트카드로부터 수신한 스마트카드의 ID인 ID_{SC}로 계산한 PI_{STB}와 스마트카드가 생성한 임의의 난수 R_{SC}를 해쉬하여 $C_1' = h(PI_{SC} \| h(h(K_{STB} \| ID_{SC}) \| R_{SC}))$를 계산하여 C_1와 C_1'가 같은지를 검증한다.

$$\begin{aligned} C_1 &= h(PI_{SC} \| h(PI_{STB} \| R_{SC}) \\ &= h(PI_{SC} \| h(h(K_{STB} \| ID_{SC}) \| R_{SC})) \\ &= C_1' \end{aligned}$$

스마트카드는 C_2를 수신한 후, 자신의 비밀키 K_{SC}와 수신한 STB의 ID인 ID_{STB}로 계산한 PI_{SC}와 STB가 생성한 임의의 난수 R_{STB}를 해쉬하여 $C_2' = h(PI_{STB} \| h(h(K_{SC} \| ID_{STB}) \| R_{STB}))$를 계산하여 C_2와 C_2'이 같은지를 검증한다.

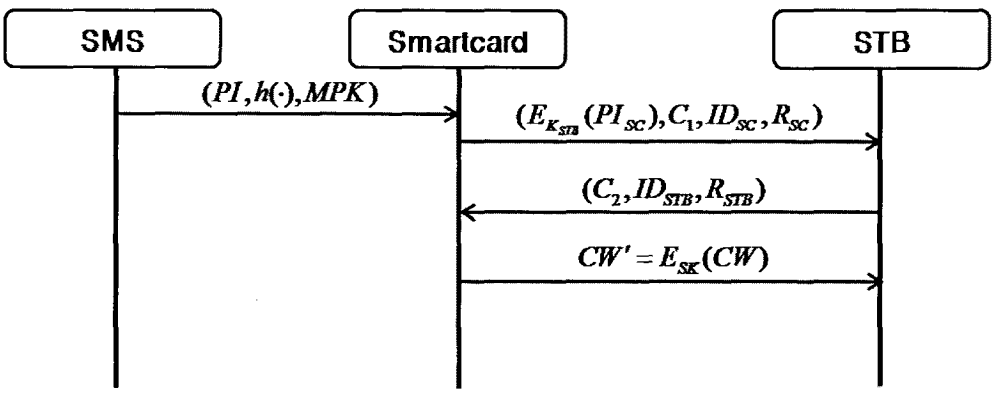


그림 4. 제안하는 프로토콜

$$C_2 = h(PI_{STB} \| h(PI_{SC} \| R_{STB})) \\ = h(PI_{STB} \| h(h(K_{SC} \| ID_{STB}) \| R_{STB})) \\ = C_2'$$

■ 키 공유 단계

상호인증 단계에서 C_1과 C_1', C_2와 C_2'이 동일한지 확인되었으면 자신이 생성했던 임의의 난수값과 상대방의 PI정보를 해쉬한 값과 자신과 상대방의 ID를 이용해 다음과 같은 세션키를 생성한다.

$$SK = h(h(PI_{STB} \| R_{SC}) \| h(PI_{SC} \| R_{STB}) \| ID_{SC} \| ID_{STB})$$

■ 제어 단어 전송 단계

스마트카드는 키 동의 단계에서 공유한 SK를 이용해 암호화된 $CW = E_{SK}(CW)$를 STB에 전송하고, STB는 공유된 SK를 이용해 $CW = D_{SK}(CW')$를 복호화하여 CW를 얻을 수 있다.

V. 분석

이 장에서는 제안하는 프로토콜이 가지는 안전성과 효율성에 대해 분석한다. 안전성 분석에 앞서 제안하는 프로토콜이 만족해야 하는 보안 요구사항들에 대해 살펴본 후 이러한 요구사항을 만족하는지에 대해 휴리스틱하게 논의한다. 효율성에 대한 분석은 3장에서 분석한 Kim이 제안한 프로토콜, Lee 등이 제안한 프로토콜과의 연산량과 메시지수를 비교하여 분석한다.

5.1 보안 요구사항

제안하는 프로토콜은 기존 논문들에서 문제가 되었던 스마트카드 복제문제, McCormac Hack 공격에 대해 안전해야 하며 추가적으로 키 동의 프로토콜의 보안 요구사항을 만족해야 한다. 제안하는 프로토콜이 만족해야 하는 보안 요구사항은 다음과 같다.

- 스마트카드 복제 문제: 적법한 사용자의 스마트카드를 복제하여 권한이 없는 사용자가 동일한 종류의 STB에서 인가된 사용자처럼 사용하는 문제이다.
- McCornmac Hack 공격: STB와 스마트카드 간의 통신 채널을 공격하여 제어 단어를 얻어낸 후, 그것을 불법적으로 사용하는 문제이다.
- 알려진 키 안전성: 공격자가 이전 세션에 생성된 세션키를 알아냈다 하더라도 그것을 이용하여 그 이전에 생성된 세션키나 앞으로 생성될 세션키를 알아내는 것이 계산적으로 어려워야 한다.
- 완전한 전방향 안전성: 공격자가 세션키 생성에 참여한 모든 개체들의 개인키를 알아냈다 하더라도 이전에 생성된 세션키를 알아내는 것이 계산적으로 어려워야 한다.
- 키 노출 저항성: 공격자가 세션키 생성에 참여한 개체 A의 개인키를 알아낸 후 다른 사용자로 위장하여 A와 프로토콜을 성공적으로 수행하는 것이 계산적으로 어려워야 한다.
- 미지의 키 공유: 개체 A와 B가 프로토콜을 수행할 때, A가 B외에 다른 개체와 키를 동의하도록 A를 속이는 것이 계산적으로 어려워야 한다.
- 키 제어: 프로토콜 수행 후 공유되는 세션키가 사전에 계산되거나 선택되어진 값이 되도록 만드는 것이 계산적으로 어려워야 한다.

5.2 안전성 분석

- 스마트카드 복제 문제: 제안하는 프로토콜에서는 사용자가 사용할 스마트카드와 STB의 ID와 비밀키는 표 3처럼 SMS에 저장되어 있다. 스마트카드와 STB는 SMS로부터 비밀통신의 대상이 될 상대방의 정보를 자신의 비밀키와 상대방의 ID가 결합되어 있는 형태로 제공받는다. 즉, 스마트카드의 경우 SMS로부터 $h(K_{STB} \| ID_{SC})$를 STB의 경우에는 $h(K_{SC} \| ID_{STB})$를 전달 받게 되는데 STB는 SMS로부터 직접 받는 것이 아니라 스마트카드를 통해 $E_{K_{STB}}(h(K_{SC} \| ID_{STB}))$형태로 전달받는다. 제안하는 프로토콜의 두 번째 단계인 상호인증단계에서 위의 두 값들을 이용하여 상대방을 인증하게 되는데 복제된 스마트카드를 다른 STB에서 사용 하고자 할 경우, STB의 ID와 비밀키가 일치하지 않아 상호인증에 실패하게 되어 시스템을 사용할 수 없게 된다. 상호인증단계에서 STB는 C_1를 통해 스마트카드를 인증하게 되는데 $C_1 = h(PI_{SC} \| h(PI_{STB} \| R_{SC}))$의 인자 중 $PI_{SC} = h(K_{SC} \| ID_{STB})$는 자신의 비밀키로 복호화하여 획득하게 된다. 이때 해당 스마트카드와 쌍을 이루는 STB가 아닌 경우 PI_{SC}를 획득하는 것은 불가능하다. 또한, $PI_{STB} = h(K_{STB} \| ID_{SC})$는 자신

의 비밀키와 스마트카드로부터 수신한 스마트카드의 ID ID_{SC}를 이용하여 계산이 가능하다. 이 과정에서 스마트카드는 자신과 비밀통신을 해야 하는 STB의 ID 정보를 이용해 값을 만들기 때문에 다른 STB와 프로토콜을 진행할 경우 올바른 값을 생성하는 것이 불가능하다. 제안하는 프로토콜은 스마트카드와 STB의 결합을 통해 스마트카드 복제 문제를 방지할 수 있다.

- McCornmac Hack 공격: 제안하는 프로토콜에서 STB와 스마트카드 사이의 통신 채널을 도청하거나 해킹을 하여도 제어 단어가 두 장치 사이의 공유된 세션키를 이용해 암호화 되어 있어 세션키를 모르는 사용자는 제어 단어를 얻어낼 수 없다. 세션키의 형태는 다음과 같다.
$SK=h(h(PI_{STB}\|R_{SC})\|h(PI_{SC}\|R_{STB})\|ID_{SC}\|ID_{STB})$
세션키 생성에 앞서 보안되지 않는 통신채널로 전달되는 값들은 $E_{K_{STB}}(PI_{SC})$, C_1, C_2, R_{SC}, R_{STB} 이다. 이 값들 중 PI_{SC}는 STB의 비밀키를 알아야만 계산할 수 있는 값이고, $h(PI_{STB}\|R_{SC})$은 STB의 비밀키를 알아야만 계산할 수 있는 값이며, $h(PI_{SC}\|R_{STB})$는 스마트카드의 비밀키를 알아야만 계산할 수 있는 값이다. 스마트카드와 STB의 비밀키는 각각의 장치에 존재하는 조작 불가능한 하드웨어에 저장되어 있기 때문에 이를 알아내는 것은 불가능하다. 따라서 제안하는 프로토콜은 McCormac Hack 공격을 방지할 수 있다.
- 위장 공격: 제안하는 프로토콜에서 스마트카드와 STB는 SMS와 사전에 공유되어 있는 각각의 비밀키 K_{SC}와 K_{STB}를 이용한 메시지를 통해 시도-응답 방식의 프로토콜을 진행하기 때문에 중간자 또는 위장자는 비밀키를 알아야만 이러한 공격이 가능하다. 그러나 이는 McCormac Hack 공격에서 보인 것처럼 비밀키를 알아내는 것이 불가능하기 때문에 위장공격에 안전하다고 할 수 있다.
- 알려진 키 안전성: 제안하는 프로토콜은 매 세션마다 임의의 난수값 R_{SC}와 R_{STB}를 사용하여 새로운 세션키를 생성한다. 임의의 난수값 R_{SC}와 R_{STB}는 보안되지 않는 통신채널을 통해 전송되기 때문에 공격자에게 쉽게 노출될 수 있다. 그러나 이 두 난수값을 안다고 해도 세션키 구성요소 중 $h(PI_{STB}\|R_{SC})$와 $h(PI_{SC}\|R_{STB})$는 스마트카드와 STB의 비밀키를 알아야만 생성이 가능하다. 하지만 비밀키를 알아내는 것은 McCormac Hack 공격에서 보인 것처럼 불가능하다. 따라서 제안하는 프로토콜은 이전에 생성된 세션키와 난수값이 노출된다 하더라도 그 이전에 생성된 세션키나 앞으로 생성될 세션키를 알아내는 것이 계산적으로 어렵다.
- 완전한 전방향 안전성: Diffie-Hellman 키 동의 프로토콜처럼 이산대수의 어려움을 이용한 키 동의 프로토콜에서 동의된 세션키의 안전성은 이산대수의 어려움에 기반한다. 즉, 이산대수 기반의 키 동의 프로토콜의 경우 개체의 개인키가 노출 된다 하더라도 세션키를 알아내기 위해선 이산대수를 풀어야 하지만 이는 계산적으로 어렵기 때문에 전방향 안정성을 보장한다고 알려져 있다. 제안하는 프로토콜은 대칭키 기반의 키 동의 프로토콜로 공유하고 있는 비밀키의 안전성이 전체 프로토콜의 안전성을 결정한다. 제안하는 프로토콜에서 개체의 개인키가 노출될 경우 이전에 생성된 세션키는 물론 현재의 세션키키도 노출되는 문제점이 존재한다. 하지만 McCormac Hack 공격에서 보인 것처럼 개체의 개인키는 조작 불가능한 하드웨어에 저장되어 있다. 이는 하드웨어의 안전성에 기반한 것으로 제안하는 프로토콜에서 개인키가 노출되는 것은 굉장히 어렵다. 대칭키 기반 프로토콜의 특성상 프로토콜만으로 전방향 안정성을 만족하지는 못하지만 프로토콜이 수행되는 환경에서 사용하는 하드웨어의 특성을 이용하여 개인키 노출을 방지 할 수 있으므로 이는 전방향 안전성에 강건하다고 할 수 있다.
- 미지의 키 공유: 스마트카드 복제 문제에서 보인 것처럼 제안하는 프로토콜은 SMS에 스마트카드와 STB의 정보가 결합되어 저장 되어있다. 프로토콜이 진행되는 동안 전달되는 모든 메시지는 두 개체의 결합정보를 바탕으로 이루어져 있다. 제안하는 프로토콜에서 스마트카드 ID_{SC_1}가 STB ID_{STB_1}를 대상으로 보내는 메시지는 ID_{STB_1}만이 복호화 할 수 있으며, ID_{SC_1}의 시도에 알맞은 응답도 ID_{STB_1}만이 할 수 있기 때문에 미지의 키 공유 조건을 만족한다.
- 키 제어: 제안하는 프로토콜에서는 세션키의 생성에 있어 모든 참여자가 프로토콜이 수행될 때

표 4. 제안하는 프로토콜의 연산량 비교

	Kim의 프로토콜	Lee 등의 프로토콜	제안하는 프로토콜
해쉬 연산	7	6	11
대칭키 암/복호화	1	1	2
지수 연산	0	4	0
XOR 연산	12	2	0
메시지 수	3	4	3

마다 임의의 난수값 R_{SC}와 R_{STB}을 이용하기 때문에 사전에 계산되거나 선택되어진 값이 세션키 생성에 영향을 끼치는 것이 불가능하다. 따라서 키 제어 조건을 만족한다.

5.3 효율성 분석

표 4는 제안하는 프로토콜과 Kim이 제안한 프로토콜, Lee 등이 제안한 프로토콜에서의 연산량과 메세지수를 나타내고 있다. 제안하는 프로토콜은 프로토콜의 경량화를 위해 연산량이 많은 지수연산의 사용을 지양하고 가벼운 연산인 해쉬와 대칭키 암호 알고리즘을 기반으로 설계하였다. 대칭키 기반 프로토콜이라 대칭키 암/복호화가 타 프로토콜들에 비해 많다. 그러나 이러한 대칭키 암/복호화는 Kim이 제안한 프로토콜에서 사용하고 있는 XOR 연산보다 안전성 측면에서 프로토콜을 보다 강건하게 한다고 할 수 있다.

VI. 결론 및 향후과제

기존 접근제한시스템에 존재하는 스마트카드 복제 문제와 McCormac Hack 공격을 해결하기 위한 스마트카드와 STB간의 안전한 키 동의 프로토콜에 대해 제안하였다. 제안하는 프로토콜은 위의 두 문제를 해결하였으며 대칭키 기반 암호알고리즘의 사용으로 기존에 이산 대수 기반으로 제안되었던 여러 프로토콜들에 비해 효율적이다. 또한 XOR연산 기반의 프로토콜에 비해 연산량이 증가 하였지만 프로토콜의 안전성 또한 증가했다고 할 수 있다.

현재까지 제안된 모든 스마트카드와 STB간의 안전한 통신을 위한 키 교환 프로토콜들에서는 하나의 스마트카드는 하나의 STB에서만 사용이 가능하다. 제안된 프로토콜 역시 그러한 제약이 존재한다. 이는 스마트카드의 복제 문제 해결을 위해 스마트카드와 STB를 결합하기 때문인데 이는 굉장히 제한적인 환경이라 할 수 있다. 향후에는 하나의 스마트카드를 동일한 접근제한시스템을 사용하는 다수의 STB에서 사용이 가능하면서도 스마트카드 복제 문제와 스마트카드와 STB간의 안전한 통신 채널을 구축 할 수 있는 부분에 대한 연구가 더 필요하다.

참고문헌

[1] EBU Project Group B/CA, "Functional model of a conditional access system," EBU Technical Review, Dec. 1995.

[2] ETSI Technical Report 289, "Support for use of scrambliong and Conditional Access within digital broadcasting system," Oct. 1996.

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

[4] http://www.irdeto.com/documents/HL_CAS_SecChip_EN_L.pdf

[5] http://www.conax.no/en/products/cas_extended/pairing/

[6] T. Jiang, Y. Hou, and S. Zheng, "Secure communication between set-top box and smart card in DTV broadcasting," IEEE Transaction on Consumer Electronics, vol. 50, no. 3, pp. 882-886, Aug. 2004.

[7] E. Yoon and K. Yoo, "A new secure key exchange protocol between STB and smart card in DTV broadcasting," Workshop on Intelligence and Security Informatics(WISI 2006), LNCS 3917, pp. 165-166, 2006.

[8] E. Yoon and K. Yoo, "Robust key exchange protocol between set-top box and smart

card in DTV broadcasting," INFORMATICA, vol. 20, no. 1, pp. 139-150, Jan. 2009.

[9] 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, Nov. 2007.

[10] 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.

[11] S. Lee, N. Park, S. Kim, and J. Choi, "Cryptanalysis of secure key exchange protocol between STB and smart card in IPTV broadcasting," International Conference on Information Security and Assurance(ISA 2009), LNCS 5576, pp. 797-803, 2009.

[12] C. Lin and T. Hwang, "A password authentication scheme with secure passwod updating," Computer & Security, vol. 22, no. 1, pp. 68-72, Jan. 2003.

[13] C. Yamg, T. Chang, and J. Li, "Security enhancement for protecting password transmission," IEICE Transaction on Communications, vol. E86-B, no. 7, pp. 2178-2181, July 2003.

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

〈著者紹介〉

이 훈 정 (Hoonjung Lee) 학생회원
2003년 2월: 단국대학교 전자컴퓨터학부(학사)
2005년 8월: 한양대학교 컴퓨터공학과(석사)
2005년 7월~2009년 6월: (주)한단정보통신 전임연구원
2009년 9월~현재: 한양대학교 컴퓨터공학과(박사과정)
〈관심분야〉 암호기술 응용, 키 관리
URL:http://infosec.hanyang.ac.kr/~hjlee

손 정 갑 (Junggab Son) 학생회원
2009년 2월: 한양대학교 전자컴퓨터공학부(학사)
2009년 3월~현재: 한양대학교 컴퓨터공학과(석사과정)
〈관심분야〉 암호기술 응용, IPTV 보안
URL:http://infosec.hanyang.ac.kr/~jgson

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과(학사)
1989년: 아이오와주립대학 전자계산학과(석사)
1992년: 아이오와주립대학 전자계산학과(박사)
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안
URL:http://infosec.hanyang.ac.kr/~hkoh/