IPTV의 미디어 서비스 보호를 위한 지문 인식 기반의 1-out-of-*n* 접근 통제 기법

정회원 이 지 선*, 이 현 숙*, 김 효 동**°

Fingerprint-Based 1-out-of-*n* Access Control Technique for Media Service Protection in IPTV Broadcasting System

Ji-Seon Lee*, Hyun Sook Rhee*, Hyo Dong Kim**° *Regular Members*

요 약

IPTV는 방송과 통신이 융합된 서비스로 송신자는 IP망을 이용하여 암호화된 콘텐츠를 멀티캐스트 방식으로 전송하고 정당한 가입자만이 인증 절차를 거친 후에 이를 복호화하여 콘텐츠를 이용할 수 있다. 이 때 가입자의 권한을 보호하기 위하여 패스워드를 기반으로 한 셋톱박스와 스마트카드 간의 인증 프로토콜이 주로 이용된다. 이 논문은 임의의 조직에서 구성원들의 지문정보를 기반으로 구성원 중 누구라도 한 사람만 있으면 암호화된 콘텐츠를 볼 수 있도록 하는 지문정보 기반의 1-out-of-n 인증 기법을 제안한다. 제안하는 기법은 패스워드와 스마트카드의 내용이 노출되더라도 정당한 지문 정보를 제공할 수 있어야만 인증받을 수 있는 디지털 방송에서 미디어 서비스 보호를 위한 지문 정보 기반의 셋톱박스와 스마트카드 간의 인증 기법이다.

Key Words : IPTV Broadcasting, Access Control, Fingerprint-based Authentication, Media Contents Protection

ABSTRACT

IPTV(Internet Protocol Television) is an emerging technology in which telecommunication and broadcasting technologies are converged. IPTV service providers usually multicast scrambled contents. And only legitimate subscribers who pass the access control can de-scramble and use the contents. In order to ensure revenues, providers oftentimes employ password-based authentication protocols that ensure secure authentication processes between set-top box and smart card. In this paper, we propose a fingerprint-based 1-out-of-n authentication protocol which provides convenient and more secure authentication process in some organizational environments. The proposed scheme shows that only those who provide legitimate fingerprint information can be authenticated even in a situation that both password and smart card are compromised.

Ⅰ. 서 론

IPTV는 초고속 광대역 네트워크를 이용해 양방향 데이터 서비스 및 디지털 영상 서비스를 TV를 통해 제공하는 대표적인 방송과 통신 융합 서비스이다. IPTV는 기존 TV의 일방적인 서비스 방식에서 벗어나 서비스 이용자가 능동적으로 TV를 시청하면서 자신이 원하는 서비스를 제공받을 수 있는 특징을 갖고 있다. 최근에는 인터넷 TV라는 장점을 최대한 이용하여 콘텐츠 제공업체들이 개인에게 초점을 맞춘 PC 기

* 고려대학교 정보경영공학전문대학원 BK21 유비쿼터스 정보보호사업단 (jslee702@korea.ac.kr, hyunsook.rhee@gmail.com)
** 아주대학교 미디어학부 (hkim@commres.org), (° : 교신저자)
논문번호 : KICS2009-12-646, 접수일자 : 2009년 12월 30일, 최종논문접수일자 : 2010년 4월 6일

반의 인터넷 콘텐츠를 가족 중심의 IPTV용 콘텐츠로 재가공시키는 추세이다. 나아가서는 개인 사용자의 편의를 위해 민원처리, 교육, 공공서비스 등이 IPTV를 통해 점점 활성화되고 있다. IPTV 이용자는 TV와 리모콘만을 이용하여 다양한 서비스를 제공받고 있으며, 이 서비스의 편의성을 증가시키기 위한 기술들이 개발, 발전되고 있는 추세이다.

IPTV에서는 멀티캐스트 방식을 이용하여 방송 콘텐츠를 전송한다. 이 기술은 하나의 송신자가 동일한 데이터를 요구하는 하나 이상의 수신자들이 속해있는 그룹에게 데이터를 동시에 전송하는 방식이다. 이 때 동일 네트워크의 가입되지 않은 사용자가 자신이 받아 볼 수 없는 콘텐츠 내용에 접근하는 것을 방지하도록 사용자를 인증하는 기법이 중요하다. 이때, 인증 절차는 셋톱박스(Set-Top Box, STB) 내에 존재하는 수신제한시스템(Conditional Access System, CAS)를 통해 이루어진다. 지금까지 제안된 인증 기법들은 스마트카드에 인증을 위해 필요한 가입자 정보가 들어있고 이 정보와 패스워드를 기반으로 셋톱박스는 인증 절차를 거친 후에, IP망을 통해서 들어오는 스크램블된 콘텐츠 신호를 복호하여 정상적인 콘텐츠로 변환하여 TV 스크린에 보여주게 된다[5,7,13,15,18]. 하지만, 패스워드는 유출되기 쉽고 스마트카드 또한 다양한 공격에 취약하다는 것이 많이 알려짐으로써 보다 안전한 인증 기법이 요구되고 있다[17]. 이에 따라 최근 들어 생체인식 기술에 많은 관심을 가지게 되었는데, 이는 사용자마다 차이가 있는 사용자 개개인의 고유한 생체정보 또는 독특한 행동 양식을 이용하여 인증하는 것으로 사용자가 기억하거나 소지할 필요가 없으므로 기존의 방법에 비해 높은 보안을 제시할 수 있다. 또한 스마트카드 리더기의 발전으로 생체 기반의 인증 방식이 더욱 주목을 받고 있는데, 최근에는 스마트카드 리더기가 자체적으로 생체 정보 템플릿 추출 및 매칭 알고리즘을 실행할 수 있도록 발전하고 있다 [2,3].

본 논문에서는 생체 정보 중에 가장 많이 이용되는 지문 정보를 이용한 스마트카드와 셋톱박스 간의 상호 인증 방식을 제안하는데, 제안하는 기법에서는 IPTV 서비스에 가입한 임의의 조직에서 구성원들 간에 패스워드와 스마트카드를 공유하고 구성원 각자가 자신만의 고유한 지문 정보를 이용하여 IPTV 서비스를 받을 수 있도록 한다. 즉, 우리가 제안하는 기법은 n명의 구성원 중 누구라도 정당한 지문 정보를 제공할 수 있는 사람이 한 명이 있으면 인증할 수 있는 기법이므로 1-out-of-n 접근 제어 기법이라고 할 수 있다. 예를 들어, 어떤 가정에서 IPTV 서비스를 받을 때 우리가 제안하는 인증 기법을 이용한다면, 가족 구성원들이 패스워드를 공유하고 구성원들의 지문 정보를 등록하여 패스워드와 스마트카드의 내용이 유출된다고 하더라도 정당하게 등록된 지문 정보를 제공할 수 있는 가족 구성원이 아니면 미디어 서비스를 받을 수 없다.

본 논문은 다음과 같이 구성된다. 2장에서는 관련된 기존 연구에 대해 간략히 서술하고, 3장에서는 본 논문에서 제안하고자 하는 셋톱박스와 스마트카드 간의 지문 정보 인증 기법의 보안 요구 사항을 정리한다. 4장에서는 스마트카드와 셋톱박스 간의 1-out-of-n 지문 기반 인증 프로토콜을 제안하고, 5장에서는 제안하는 프로토콜이 다양한 공격에 안전함을 보인다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

셋톱박스 내의 수신제한시스템은 시청권한을 가진 가입자만이 특정 프로그램을 수신할 수 있게 해 주는 서브시스템으로 방송사업자의 수익을 보호하고 시청자 위주의 방송 편성을 가능하게 해 준다. 방송 송신 측은 제공하는 미디어 콘텐츠를 암호화하여 전송하고 수신 측에서는 시청 권한을 가진 가입자만이 셋톱박스 내의 수신제한시스템을 이용하여 인증 과정을 거쳐 암호화된 콘텐츠를 복호화하여 볼 수 있어야 한다. 이 때 중요한 것이 가입자 비밀키와 스마트카드인데, 가입자 관리 시스템(Subscriber Management System, SMS)이 가입자 비밀키(Master Private Key, MPK)와 스마트카드를 관리한다. 일반적으로 가입자 비밀키는 가입자가 최초로 가입하는 시점에 가입자 관리 시스템에 의해 관련 비밀 정보들과 함께 스마트카드 안에 내장되어 가입자에게 배포된다. 방송 송신 측의 콘텐츠 암호화 과정(스크램블링)과 수신측의 복호화 과정(디스크램블링)은 다음과 같다 [9](그림 1).

(1) MPK를 사용해서 인증키(Authorization Key, AK)를 암호화하여 자격 관리 메시지 (Entitlement Management Message, EMM)를 통해 전송한다.

(2) AK를 이용하여 제어 단어(Control Word, CW)를 암호화하여 자격 제어 메시지 (Entitlement Control Message, ECM) 형태로 전송한다.

(3) 암호화된 미디어 콘텐츠인 전송 스트림(TS), ECM, EMM이 멀티캐스트된다.

(4) 수신측에서는 스마트카드에 저장된 MPK로 EMM을 복호화하여 AK를 알아낸다.

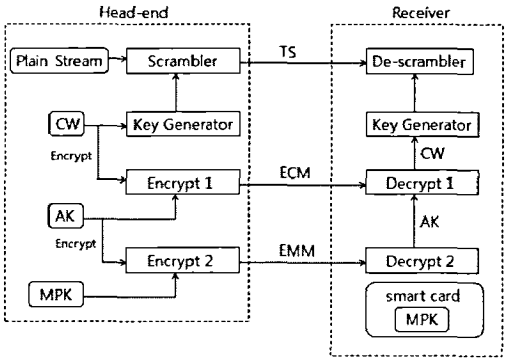


그림 1. 수신제한시스템 (CAS: Conditional Access System)

(5) AK를 이용하여 ECM을 복호화하고 CW를 알아낸다.

(6) 이 과정에서 스마트카드와 셋톱박스는 안전하게 CW를 주고받기 위하여 공유키 SK를 생성하고, 스마트카드는 CW를 SK로 암호화하여 셋톱박스로 보낸다. 암호화된 CW를 받은 셋톱박스는 SK를 이용하여 CW를 복호화한다. 마지막으로 복호화된 CW를 이용하여 TS를 복호화하여 원래 콘텐츠를 가입자에게 보여준다.

위의 과정에서 MPK는 SMS에 의해 관리되고, SMS는 수신제한시스템 내의 가입자 권한 시스템(Subscriber Authorization System, SAS)에 요청을 보내어 가입자 정보를 등록, 수정, 삭제한다. SAS는 유료 TV 프로그램 정보, 스마트카드의 ID 번호 등과 같은 정보들로 이루어진 데이터베이스를 구축한다. 일반적으로 가입자 관련 비밀 정보들은 스마트카드 안에 내장되어 SMS를 통해 가입자에게 배포된다.

2.1. 스마트카드와 셋톱박스 간의 상호 인증 기법 관련 기존 연구와 보안 요구 사항

2004년 Jiang-Hou-Zheng이[7] 스마트카드와 셋톱박스 간의 상호 인증 기법을 제안한 이래로 다수의 기법들이 여러 논문에서 제안되었다 [5,13,15,18]. 스마트카드와 셋톱박스 사이에 가능한 공격 기법으로는 다음과 같이 맥코맥 핵 공격 (McCormac Hack Attack)과 스마트카드 복제 공격 (Smart Card Cloning Attack)이 있는데 이 두 공격은 모두 정당하지 않은 스마트카드를 셋톱박스가 정당한 스마트카드로 인지하도록 하려는 공격이다 [8]. 맥코맥 핵 공격 (McCormac Hack Attack)은 스마트카드로부터 셋톱박스로 연결되는 데이터 라인을 같은 종류의 다른 셋톱박스로 전송하여 접근허가를 받으려는 공격이다. 스마트카드 복제 공격 (Smart Card Cloning Attack)은 정당한 스마트카드를 복제하여 복제된 카드를 다른 셋톱박스에 넣어서 접근허가를 받으려는 공격이다.

또한 일반적인 상호 인증 기법에서와 같이 스마트카드와 셋톱박스 간의 인증 기법에서도 재전송 공격 (Replay Attack)과 중간자 공격(Man-In-The-Middle Attack)에 대한 안전성을 보장해야 한다.

2.2 지문 기반 인증 기법 관련 기존 연구와 보안 요구 사항

지문 기반 인증 기법은 2002년 Lee-Ryu-Yoo[14]가 2개의 비밀키와 공개키 암호 시스템을 이용하여 제안한 이래로 다수의 기법들이 제안되었다. 2004년에는 Lin-Lai[16]가 Lee-Ryu-Yoo의 기법이 위조 공격에 안전하지 않음을 보이고 보다 개선된 기법을 제안하였다. 하지만, Khan-Zhang[10]에 Lin-Lai의 기법 또한 안전하지 않음이 알려졌고, 2008년에 Khan-Zhang-Wang[11]에 의해 새로운 해쉬 기법에 기반을 둔 지문 기반 인증 기법이 제안되었다. 이외에도 다양한 지문 기반 인증 기법이 제안되고 분석되었다 [6,12].

지문 기반 인증은 기존의 스마트카드와 패스워드만으로 인증이 이루어졌던 것과 달리 지문 정보가 하나 더 들어감으로써 정당치 않은 사용자가 세 개 중에 어느 두 가지의 정보만을 가지고 접속을 시도하려고 해도 불가능해야 한다. 따라서 스마트카드를 가지고 있고, 패스워드를 알고 있으면서 올바른 지문 정보를 제공할 수 있는 정당한 가입자만이 정보에 접근할 수 있어야 한다. 하지만 이러한 기존의 지문 기반 인증 기법들은 모두 서버-클라이언트 모델에서의 인증 기법으로 패스워드와 스마트카드만을 가지고 인증을 수행하던 기존 연구에 비해 지문 인식을 추가한 보다 보안을 강화시킨 연구 결과들이라는데 의미가 있다.

최근에 IPTV방송 환경에서의 인증 기법 중 하나로 속성 기반 인증 기법이 제안되었는데[4], 이 기법에서는 패스워드와 스마트카드 외에 각 개인이 가지고 있는 속성을 기반으로 인증하는 기법이었다. 따라서 제안된 기법은 여전히 두 가지 요소 (패스워드, 스마트카드)를 이용한 인증 기법이고, 본 논문에서 제안하고자 하는 기법은 IPTV 환경에서 n명 중 1명이라도 올바른 지문 정보를 제공할 수 있는 사용자가 있어야만 인증받을 수 있는 기법으로 세 가지 요소(패스워드, 스마트카드, 지문 정보)를 제공해야만 인증이 성립하는 기법이다.

Ⅲ. 스마트카드와 셋톱박스 간의 지문 정보 기반 1-out-of-*n* 인증 기법의 보안 요구 사항

본 논문에서 제안하고자 하는 지문 정보 기반의 1-out-of-*n* 인증 기법은 *n*명으로 구성된 임의의 그룹에서 *n* 명 중 1명이 옳은 정보(패스워드, 스마트카드, 지문정보)를 제공하면 인증이 성립하는 기법이다. 즉, 구성원 중 누구라도 패스워드와 스마트카드를 공유하고 자신의 지문 정보를 이용하여 인증이 가능하다. 이 기법은 가족과 같은 조직에서 IPTV 서비스를 받아보기에 적합한 기법인데, 가족들끼리 패스워드와 스마트카드를 공유하고 가족 구성원 중에 누구라도 자신만의 지문 정보를 이용하여 인증을 하고 원하는 서비스를 받아볼 수 있다. 따라서 패스워드와 스마트카드의 내용이 유출된다고 하더라도 가족 구성원 중의 누구라도 있어야만 인증에 성공할 수 있다. 이 때 중요한 보안 요구 사항은 다음과 같다.

(1) 맥코맥 핵 공격에 대한 안전성 : 스마트카드로부터 셋톱박스로 연결되는 데이터 라인을 같은 종류의 다른 셋톱박스로 전송하여 접근허가를 받으려는 공격에 안전해야 한다.

(2) 스마트카드 복제 공격에 대한 안전성 : 정당한 스마트카드를 복제하여 복제된 카드를 다른 셋톱박스에 넣어서 접근허가를 받으려는 공격에 안전해야 한다.

(3) 재전송 공격(Replay Attack)에 대한 안전성 : 프로토콜 상에서 유효한 메시지를 골라 저장해 두었다가 나중에 재전송함으로써 정당한 사용자로 가장하는 공격에 안전해야 한다.

(4) 중간자 공격(Man-In-The-Middle Attack)에 대한 안전성 : 셋톱박스와 스마트카드 간의 통신 메세지를 공격자가 중간에서 도청하거나 자신이 변조한 메시지로 통신내용을 바꾸는 공격에 대하여 안전해야 한다.

(5) 오프라인 패스워드 추측 공격(Offline Password Guessing Attack)에 대한 안전성 : 셋톱박스와 스마트카드 간의 통신 메시지들을 모두 갖고, 조직원들의 지문 정보와 스마트카드의 내용이 유출된다고 하더라도 조직의 패스워드를 알아낼 수 없어야 한다.

(6) 패스워드와 스마트카드 노출에 대한 안전성 : 패스워드와 스마트카드의 내용이 노출된다고 하더라도 정당한 지문 정보를 제공할 수 없으면 인증이 성립할 수 없어야 한다.

Ⅳ. 스마트카드와 셋톱박스 간의 지문 정보 기반 1-out-of-*n* 인증 기법

이번 장에서는 지문 인식 기반의 인증 기법을 제안한다. 우선 본 논문에서 사용되고 있는 각 용어를 정리하겠다.

- ID_i, PW_i: 사용자의 아이디, 패스워드
- ID_S : 셋톱박스의 고유 일련 번호 (셋톱박스의 아이디)
- x_S : 셋톱박스의 비밀키
- $E_k(\cdot)/E_k^{-1}(\cdot)$: 대칭키 k를 이용한 암호/복호 알고리즘
- l : 보안 파라미터
- p : 512비트의 소수
- $h(\cdot): \{0,1\}^* \rightarrow \{0,1\}^l$: 일방향 해쉬 함수
- $\|$: concatenation 연산자
- $\oplus$: bitwise exclusive-or 연산자

4.1 등록 단계

(1) 새로운 사용자 그룹 U_i는 아이디 ID_i와 패스워드 PW_i를 선택한다. 다음으로 그룹의 각 구성원들의 지문을 입력하여 지문 템플릿 집합 $S_i = \{s_{i,1}, s_{i,2}, \cdots, s_{i,n}\}$을 구성한다. 다음으로 임의의 난수 $r \in Z_p^*$을 선택하여 $s_{i,j}^* = s_{i,j} \oplus r, (1 \le j \le n)$, 을 계산한 후 집합 $S_i^* = \{s_{i,1}^*, s_{i,2}^*, \cdots, s_{i,n}^*\}$을 구성한다. U_i는 ID_i, PW_i, S_i^*를 안전한 채널을 통해 가입자 관리 시스템에 전달한다. 여기에서 안전한 채널이란 공격자가 접근할 수 없는 안전하게 자료를 전달할 수 있는 통로를 말한다. (그룹 구성원을 n명이라 가정하고, ID_i와 PW_i를 선택하고 스마트카드 발급에 관여하는 그룹의 대표를 가정하자. 이후로는 다른 그룹

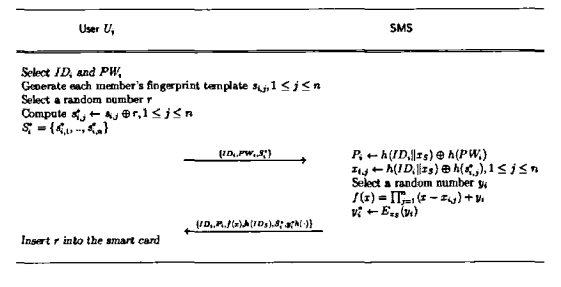


그림 2. 등록 단계

구성원들과 똑같이 인증 과정을 진행한다. 또한 지문 템플릿 집합을 구성하기 위해서는 모든 구성원이 자신의 지문을 등록해야 한다.)

(2) 가입자 관리 시스템은 U_i로부터 받은 ID_i, PW_i, S_i^*와 셋톱박스의 비밀 키 x_S를 이용하여 다음을 계산한다.

$$P_i = h(ID_i \parallel x_S) \oplus h(PW_i)$$

$$x_{i,j} = h(ID_i \parallel x_S) \oplus h(s_{i,j}^*), 1 \le j \le n$$

(3) 임의의 난수 $y_i \in Z_p^*$를 선택하고, 위에서 계산한 $x_{i,j}(1 \le j \le n)$ 값들을 이용하여 다음과 같이 다항식 $f(x)$를 구하고, y_i를 셋톱박스의 비밀키 x_S를 이용하여 암호화하여 y_i^*를 구한다.

$$f(x) = \prod_{j=1}^{n}(x - x_{i,j}) + y_i$$

$$y_i^* = E_{x_S}(y_i)$$

(4) 가입자 관리 시스템은 스마트카드에 $\{ID_i, P_i, f(x), h(ID_S), S_i^*, y_i^*, h(\cdot)\}$를 저장하고 U_i에게 전송한다. 여기에서 $h(ID_S)$는 셋톱박스의 고유 일련번호에 해쉬 함수를 취하여 얻은 값으로 스마트카드와 셋톱박스만이 알고 있는 값이다. 즉, 스마트카드는 ID_S는 모르지만 $h(ID_S)$ 값을 알고 있다. 또한 해쉬 함수 $h(\cdot)$도 비밀 정보이다.

(5) 스마트카드를 받은 U_i는 임의로 선택했던 정수 r을 스마트카드에 입력한다.

4.2 로그인 및 상호 인증 단계

조직의 구성원 중 누구라도 IPTV를 시청하고자 할 때 자신의 지문을 스캔하여 템플릿 $s_{i,j}$을 구한다. 다음으로 스마트카드는 $s_{i,j}^* = s_{i,j} \oplus r$을 계산하여 $s_{i,j}^*$이 집합 S_i^*에 존재하는지 확인한다. 만약에 존재하지 않는다면 로그인 요청을 받아들이지 않고, 존재한다면 패스워드 PW_i를 입력하여 다음 과정을 수행한다.

(1) 스마트카드는 우선 $K = P_i \oplus h(PW_i)$를 계산하고 $x_{i,j} = K \oplus h(s_{i,j}^*)$를 구한 후 $f(x_{i,j})$ 값을 구한다. 구한 $f(x_{i,j})$ 값은 y_i가 된다. 스마트카드는 임의의 정수 $a \in Z_p^*$를 선택하여 $A = h(K \parallel y_i) \oplus a$를 계산한다. 또한 $y_i^{**} = K \oplus y_i^*$를 구한다.

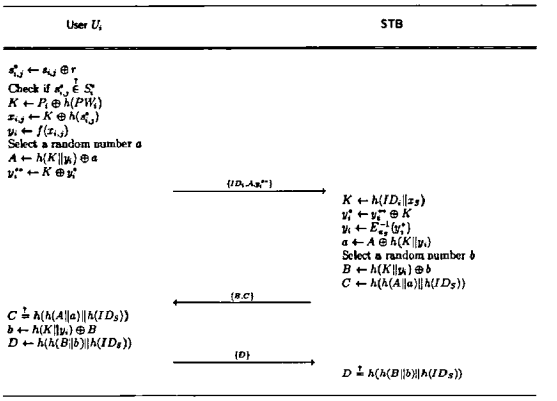


그림 3. 상호 인증 단계

(2) U_i는 $\{ID_i, A, y_i^{**}\}$를 셋톱박스로 보낸다.

(3) $\{ID_i, A, y_i^{**}\}$을 받은 셋톱박스는 $K = h(ID_i \parallel x_S)$를 계산하여 $y_i^* = y_i^{**} \oplus K$ 구하고 y_i^*를 복호하여 $y_i = E_{x_S}^{-1}(y_i^*)$를 얻는다. 다음으로 $a = A \oplus h(K \parallel y_i)$를 구한 후 임의의 수 $b \in Z_p^*$을 선택하여 $B = h(K \parallel y_i) \oplus b$를 계산한다. 또한 셋톱박스는 $C = h(h(A \parallel a) \parallel h(ID_S))$를 계산한다.

(4) 셋톱박스는 $\{B, C\}$를 U_i에게 보낸다.

(5) U_i는 C와 $h(h(A \parallel a) \parallel h(ID_S))$가 같은 값을 갖는지 확인한다. 만약에 둘이 같다면, U_i는 셋톱박스를 인증하고 다음 단계를 수행한다. 둘이 같지 않다면 U_i는 더 이상 인증 과정을 수행할 수 없다.

(6) 셋톱박스를 인증한 U_i는 $b = h(K \parallel y_i) \oplus B$를 구하여 $D = h(h(B \parallel b) \parallel h(ID_S))$를 계산한 후 D를 셋톱박스로 보낸다.

(7) 셋톱박스는 $h(h(B \parallel b) \parallel h(ID_S))$를 계산하여 받은 D와 같은지 확인한다. 만약에 두 값이 같다면 셋톱박스는 사용자 U_i를 인증하게 되고, U_i와 셋톱박스 간에 상호 인증이 이루어진다.

4.3 제어 단어 전달 단계

상호 인증이 성립하면, 스마트카드와 셋톱박스는 공유키 $SK = h(a, b, ID_i, h(ID_S))$를 계산하여 제어 단어 전달에 이용한다.

(1) 스마트카드는 가입자 비밀키 MPK를 이용하여

제어 단어를 복호화해내고, 계산한 공유키 SK를 이용하여 제어 단어를 암호화하여 셋톱박스에 보낸다.

(2) 셋톱박스는 암호화된 제어 단어를 공유키 SK를 이용하여 제어 단어를 복호화해서 원하는 콘텐츠를 디스크램블링한다.

V. 제안하는 프로토콜의 보안 분석

이번 장에서는 4장에서 제안한 기법이 3장의 보안 요구 사항을 만족함을 보이겠다.

(1) 맥코맥 핵 공격에 대한 안전성 : 공격자가 스마트카드로부터 셋톱박스로 연결되는 데이터 라인을 같은 종류의 다른 셋톱박스로 전송하여 접근 허가를 받으려고 시도한다고 가정하자. 이 때 인증이 성공하기 위해서는 공격을 시도하는 셋톱박스의 유일한 식별자인 ID_S를 알아야 하는데, 스마트카드가 가지고 있는 ID_S는 셋톱박스가 갖는 비밀값으로 유지되는 유일한 식별자이기 때문에 다른 식별자를 갖는 셋톱박스와는 맥코맥 핵 공격을 이용하여 인증에 성공하는 것이 불가능하다.

(2) 스마트카드 복제 공격에 대한 안전성 : 정당한 스마트카드를 복제하여 자신이 이용할 수 없는 셋톱박스에 넣어서 접근 허가를 얻어내려는 공격이다. 하지만 맥코맥 핵 공격에서와 같이 각 셋톱박스가 자신의 고유한 식별자 ID_S와 비밀키 x_S를 가지고 있기 때문에 스마트카드 복제 공격에도 안전하다.

(3) 재전송 공격(Replay Attack)에 대한 안전성 : 우리가 제안하는 기법에서는 재전송 공격에 이용될 수 있는 A, B, C, D 값이 매 세션마다 다른 임의의 난수 a 또는 b를 포함하기 때문에 재존송 공격에 안전하다.

(4) 중간자 공격(Man-In-The-Middle Attack)에 대한 안전성 : 제안하는 기법에서 공격자가 중간자 공격에 성공하기 위해서는 스마트카드가 셋톱박스를 인증하도록 하기 위해 스마트카드가 받아들일 수 있는 B와 C 값을 계산해야 한다. 하지만, 공격자가 x_S 없이 K와 y_i를 계산할 수 없고 따라서 B를 옳게 계산할 수 없다. 또한 임의의 난수 a와 ID_S 없이는 스마트카드가 받아들일 수 있는 C 값을 계산하는 것 역시 불가능하다.

(5) 오프라인 패스워드 추측 공격(Offline Password Guessing Attack)에 대한 안전성 : 우리가 제안하는 기법에서는 공격자가 셋톱박스와 스마트카드 간의 통신 메시지들을 모두 갖고, 조직원들의 지문 정보인 지문 템플릿 집합 $S_i = \{s_{i,1}, s_{i,2}, \cdots, s_{i,n}\}$와 스마트카드의 내용을 안다고 하더라도 조직의 패스워드를 추측해낼 수 없다. 왜냐하면, 패스워드를 추측하기 위해서는 스마트카드가 계산해야 하는 식 $K = P_i \oplus h(PW_i)$에서 추측 가능한 패스워드를 넣어 보고 등식이 성립하는지를 확인해야 하는데, P_i는 스마트카드 안에 있는 값이지만 K 값을 알기 위해서는 x_S가 필요하다. 하지만 이 값은 셋톱박스만이 알고 있는 비밀키이므로 패스워드를 추측해낼 수 없다.

(6) 우리가 제안하는 기법은 패스워드와 스마트카드의 내용이 노출된다고 하더라도 정당한 지문 정보를 제공할 수 없으면 인증이 성립할 수 없다. 공격자에게 PW_i와 스마트카드의 내용 $\{ID_i, P_i, f(x), h(ID_S), S_i^*, y_i^*, h(\cdot)\}$이 노출된다고 가정하자. 공격자는 인증에 성공하기 위하여 셋톱박스가 인증할 수 있는 $\{ID_i, A, y_i^{**}\}$를 계산하려고 할 것이다. 이 때 공격자는 $K = P_i \oplus h(PW_i)$를 계산할 수 있기 때문에 y_i^{**}를 계산할 수 있다. 하지만, $A = h(K \| y_i) \oplus a$를 계산하려면 y_i를 계산할 수 있어야 하는데, y_i를 구하기 위해서는 지문 정보 $s_{i,j}^*$를 구해서 $x_{i,j} = K \oplus h(s_{i,j}^*)$를 계산해야 한다. 따라서 정당한 지문 정보를 제공할 수 없다면 패스워드와 스마트카드의 내용을 알더라도 셋톱박스가 받아들일 수 있는 정당한 A를 구할 수 없다.

VI. 결 론

최근 들어 강화된 보안을 위하여 지문 인식 기술에 많은 관심을 가지게 되었고, 여기에 더하여 스마트카드 리더기의 발전으로 스마트카드 기반의 지문 기반 인증 방식이 더욱 주목을 받고 있다. 본 논문에서는 IPTV에서 임의의 조직에서 구성원들의 지문 정보를 기반으로 구성원 중 누구라도 한 사람만 있으면 암호화된 콘텐츠를 볼 수 있도록 하는 지문 정보 기반의 1-out-of-n 인증 기법을 제안하였다. 즉, n명의 구성원들이 패스워드와 스마트카드는 공유하고 각자 자신의 지문 정보를 등록하여 정당한 패스워드와 스마트카드 뿐 아니라 n명 중 한 명의 옳은 지문 정보를 제공해야만 콘텐츠 접근에 성공할 수 있는 기법이다. 따라서 본 논문에서 제안한 패스워드, 지문 정보, 그리고 스마트카드를 기반으로 한 1-out-of-n 인증 기법은 디지털 방송에서 가입자의 권리와 미디어 서비스 제공업체의 이익을 보호할 수 있는 기술로 실제 생활에 적용될 수 있을 것으로 기대한다.

하지만 본 논문에서 제안한 IPTV에서의 1-out-ot-*n* 인증 기법은 기존의 보안 요구 사항에 따른 보안 분석만으로 안전도를 증명하고 있다. 이와 관련하여 앞으로 IPTV 환경에서 시뮬레이션 등을 통하여 제안하는 기법이 안전함을 보일 수 있도록 한다면 보다 개선된 기법을 설계하고 분석하는데 도움이 될 것이다. 따라서 시뮬레이션을 통한 보안 분석이 추후에 연구되어야 할 부분 중 하나이다.

참 고 문 헌

[1] 박종열, 문진영, 백의현, "IPTV 융합 서비스를 위한 보안 기술 동향," 전자통신동향분석 제23권, 제5호, 2008년 10월.

[2] 반성범, 정용화, 김호원, 박영수, "IC 카드를 이용한 생체인식 기술 개발 동향," 정보과학회지, 제9권, 제7호, 2001년 7월.

[3] 심규호, "삼성전자, 스마트카드 칩 국제 보안인증 획득," 전자신문 2007. 4. 27.

[4] 이지선, 김효동, "IPTV방송 시스템에서의 속성 기반 사용자 인증 기법," 방송공학회논문지, 제14권, 제3호, 2009년 5월.

[5] T-W. Hou, J.-T. Lai and C.-L. 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.

[6] B.T. Hsieh, H.Y. Yun, H.M. Sun and C.T. Lin, "Cryptanalysis of a fingerprint-based remote user authentication scheme using smart cards," Proceedings of 37th IEEE conference on security technology, pp.349-350, 2003.

[7] 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, August, 2004.

[8] F. Kamperman and B.V. Rijnsoever, "Conditional access system interoperability through software downloading", IEEE Trans. On Consumer Electronics, Vol.47, No.1, pp.47-53, 2001.

[9] W. Kanjanarin and T. Amomraksa, "Scrambling and Key Distribution Scheme for Digital Television," IEEE International Conference on Networks, pp.140-145, Oct. 2001.

[10] M.K. Khan and J. Zhang, "Improving the security of a flexible biometrics remote user authentication scheme," Computer Standards and Interfaces, Vol.29, No.1, pp.82-85, 2007.

[11] M.K. Khan, J. Zhang and X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," Chaos, Solitons and Fractals, Vol.35, No.3, pp. 519-524, 2008.

[12] W.C. Ku, S.T. Chang, and M.H. Chiang, "Further cryptanalysis of fingerprint-based remote user authentication scheme using smart cards," Electronics Letters, 41(5), pp.240-241, 2005.

[13] S.-H. Lee, N.-S. Park, S.-K. Kim and J.-Y. Choi, "Cryptanalysis of Secure Key Exchange Protocol Between STB and Smart Card in IPTV Broadcasting," ISA 2009, LNCS 5576, pp.797-803, 2009.

[14] J.K. Lee, S.R. Ryu and K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electronics Letters, 38(12), pp.554-555, 2002.

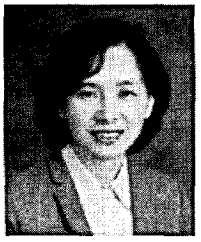
[15] J.S. Lee, H.S. Rhee, and D.H. Lee, "Efficient and Secure Communication between Set-top Box and Smart Card in IPTV Broadcasting," IEEE International Conference on Convergence and Hybrid Information Technology, pp.307-310, Aug. 2008.

[16] C.H. Lin and Y.Y. Lai, "A flexible biometrics remote user authentication scheme," Computer Standards & Interfaces, 27(1), pp.19-23, 2004.

[17] T.S. Messergers, E.A. Dabbish, and R.H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers 51(5), pp.541-552, 2002.

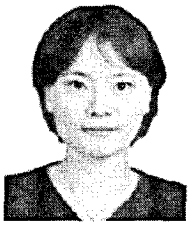
[18] E.-J. Yoon and K. Yoo, "Robust Key Exchange Protocol between Set-top Box and Smart Card in DTV Broadcasting," Informatica 20(1), pp.139-150, 2009.

이 지 선 (Ji-Seon Lee) 정회원



1991년 2월 서강대학교 전자계산학과
1998년 8월 서강대학교 컴퓨터공학과 석사
2008년 2월 서강대학교 컴퓨터공학과 박사
2008년 3월~현재 고려대학교 BK21유비쿼터스 정보보호사업단 연구 교수
<관심분야> 암호학, 네트워크 보안, IPTV 보안

이 현 숙 (Hyun Sook Rhee) 정회원



1998년 2월 단국대학교 수학과
2000년 2월 단국대학교 응용수학 석사
2008년 2월 고려대학교 정보경영공학전문대학원 정보보호전공 박사
2008년 3월~2008년 8월 고려대학교 정보경영공학전문대학원, 박사후 연구원
2008년 9월~2009년 3월 Univ. of Wollongong(호주), 박사후 연구원
2009년 6월~현재 고려대학교 BK21유비쿼터스 정보보호사업단 연구 교수
<관심분야> 정보보호, PET 기술, IPTV와 Smart Card 관련 보안 기술 등.

김 효 동 (Hyo Dong Kim) 정회원

1992년 2월 서강대학교 사학과
1997년 5월 : University of Utah, Communications 석사
2003년 1월 Rutgers University, Communications 박사
2004년~현재 아주대학교 미디어학부 부교수
<관심분야> 커뮤니케이션 테크놀로지, 디지털방송