DOI: 10.3745/KIPSTC.2010.17C.4.347

다운로드형 수신제한시스템(XCAS)에 적합한 PKI기반의 장치 인증기법에 대한 연구

황 유 나[†] · 정 한 재[††] · 원 동 호[†††] · 김 승 주[††††]

요 약

수신제한시스템이란 정당한 사용자만이 방송 콘텐츠에 접근할 수 있도록 하는 하드웨어 기반 시스템이다. 수신제한시스템의 경우에는, 방송 사업자 교체 시 셋탑 박스를 교체해야 한다는 점, 스마트카드에 의한 빈번한 오작동과 같은 문제점이 있었다. 이러한 문제점을 해결하기 위해 2009년에 XCAS가 개발되었다. 그러나, XCAS에서는 적합한 셋탑 박스(Set-top box)를 인증하기 위한 방식이 제안된 바 없다. 따라서, 본 논문에서는 XCAS에서의 새로운 인증 방식을 제안하고자 한다. 또한 XCAS에 적합한 인증서 구조 및 방송 서비스를 위한 인증서 발급 절차를 제안한다. 제안 하는 셋탑 박스 인증기법은 MSO에서 셋탑 박스 인증시에 2개의 주체 간에만 통신하도록 구성 되어 효율성이 높다.

키워드 : XCAS, Exchangeable CAS, 장치인증, PKI, DCAS, Downloadable CAS

A Study on Appropriate Device Authentication Scheme Based PKI for Exchangeable CAS (XCAS)

Yu-na Hwang[†] · Hanjae Jeong[††] · Dongho Won[††††] · Seungjoo Kim[†††††]

ABSTRACT

A condition access system (CAS) refers to a hardware-based system that allows only authenticated users to have access to contents. The CAS has many disadvantages found in that in the replacement of multiple service operator (MSO) a set-top box should be also changed and the smart-card often causes malfunction. To deal with the problems, exchangeable CAS (XCAS) was developed in 2009. However, in the XCAS, no method to authenticate a proper set-top box has been put forward. In this paper, we propose a novel program for set-top authentication in the XCAS. Additionally, we offer a format of certificate of authentication, and procedures of issuing the certificate for broadcasting services suitable for the XCAS. The technical method of authentication a set-top box that will be discussed is of high efficiency since in the MSO it requires only two subjects to communicate during the authentication in the MSO.

Keywords : XCAS, Exchangeable CAS, Device Authentication, PKI, DCAS, Downloadable CAS

1. 서 론

위성 혹은 케이블 방송 시스템에서 유료 채널을 관리하며 불법적인 사용자의 시청을 방지하는 기술은 해당 사업자의 수익성과 직접적으로 연관된다. 이와 관련하여 정당한 사용자만 방송 콘텐츠(contents)에 접근하도록 하는 기술을 하드웨어를 기반으로 구현한 것을 수신제한시스템(CAS, Conditional Access System)이라고 한다. 현재 유료 방송 시스템에서는 수신제한시스템이 사용되고 있다. 그러나 수신제한시스템은 인증 및 디스크램블 과정을 하드웨어 장치를 기반으로 처리하기 때문에 몇 가지 문제점을 가지고 있다. 이러한 수신제한시스템의 문제점을 해결하기 위하여 제안된 시스템이 다운로드형 수신제한시스템(XCAS, Exchangeable CAS)이다. 국외에서는 미국을 중심으로 수신제한시스템을 DCAS(Downloadable CAS)로 대체 하려는 움직임이, 국내에서는 XCAS로 대체하려는 움직임이 가속화되고 있다. 그러나 현재까지 XCAS를 사용하기 위해서 셋탑 박스를 인증하는데 적용될 수 있는 인증기법이 없다. 따라서 XCAS에 적합한 셋탑 박스 인증기법이 필요하다.

본 논문에서는 현재 소개되어 있는 공개키 기반 장치 인증기법을 분석하고 XCAS를 위한 장치 인증기법에 대하여

※ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(계약번호 UD100002KD)
본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2010-(C1090-1031-0005))
† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 석사과정
†† 준 회 원 : 성균관대학교 휴대폰학과 박사과정
††† 종신회원 : 성균관대학교 정보통신공학부 교수
†††† 종신회원 : 성균관대학교 정보통신공학부 교수(교신저자)
논문접수 : 2010년 4월 21일
수 정 일 : 1차 2010년 6월 21일, 2차 2010년 7월 21일
심사완료 : 2010년 7월 26일

제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 XCAS와 공개키 기반 장치 인증기법을 분석한다. 3장에서는 XCAS에 적합한 PKI(Public Key Infrastructure) 기반의 장치 인증기법에서 고려되어야 하는 성능 및 보안 요구사항을 도출하고, XCAS에 적합한 PKI 기반의 장치 인증을 제안한다. 4장에서는 본 논문에서 제안하는 셋탑 박스 인증절차에 대한 효율성과 안전성을 분석한다. 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

2.1 다운로드형 수신제한시스템(XCAS) 분석

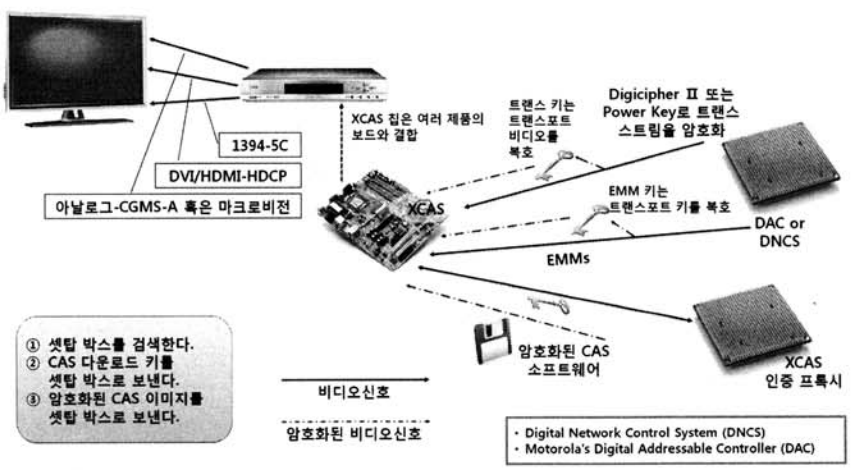
수신제한시스템은 방송 사업자가 전송하는 방송 콘텐츠를 요금을 지불한 가입자의 단말기에서만 이용할 수 있도록 하는 방송 서비스용 수신제한시스템이다. 수신제한시스템은 방송 사업자가 비밀번호를 생성하고 생성된 비밀번호를 기반으로 방송 콘텐츠를 스크램블하여 전송한다. 스크램블된 콘텐츠는 비밀번호를 알고 있는 사용자만 스크램블을 제거하여 정상적인 방송을 수신할 수 있다. 수신제한시스템의 동작과정은 다음과 같다[1-4, 19].

(1) 서버는 제어단어생성기(CWG, Control Word Generator)에서 생성한 제어단어(CW, Control Word)를 이용하여 스크램블된 방송 콘텐츠를 수신자에게 전송
(2) CW는 서버의 인증키(Service Key)를 이용하여 자격제어메시지(ECM, Entitlement Control Message)로 변환되어 전송
(3) 인증키는 가입자관리시스템(SMS, Subscriber Management System)에 의해 관리 및 배포되는 가입자 비밀키(Secret Key, 스마트카드에 탑재)를 통해 자격관리메시지(EMM, Entitlement Management Message)로 변환되어 전송
(4) 수신자는 자신의 비밀키를 이용하여 서버의 인증키를 복호화
(5) 수신자는 복호화된 서버의 인증키를 이용하여 CW를 복호화한 뒤 수신된 데이터를 디스크램블링

이와 같은 방법을 사용하기 위해 셋탑 박스에 비밀번호를 저장한 칩을 내장하거나, 스마트카드를 셋탑 박스에 삽입하는 방법을 이용한다. 그러나 이와 같은 방법은 사용자가 방송 사업자를 옮기게 될 경우, 셋탑 박스 자체를 바꾸거나 스마트카드를 교체해야 한다는 문제점이 있다. 스마트카드의 경우, 셋탑 박스를 변경하는 방법보다 진보한 방법이지만 스마트카드에서 발생하는 열에 의하여 셋탑 박스가 오동작하는 문제점이 발생하였다[1-4, 19]. 따라서, 이러한 문제점을 해결하고자 새로운 개념의 수신제한시스템으로 다운로드형 수신제한시스템(Exchangeable CAS, XCAS)이 등장하였다. XCAS의 일반적인 시스템 구조는 (그림 1)과 같다.

기존 시스템이 하드웨어 칩이나 스마트카드를 이용한 하드웨어 기반의 사용자 인증 방식을 사용하는데 반해, XCAS는 적절한 소프트웨어를 다운로드 및 설치하여 이를 활용한다. 소프트웨어를 다운로드 받기 위해서는 방송사업자(MSO, Multiple Service Operator)와 통신을 해야 하며, 이 때 발생하는 통신에 대한 보안 및 안전한 소프트웨어의 다운로드를 위하여 기존 수신제한시스템에 비해 훨씬 높은 강도의 보안성을 필요로 한다[1-4, 19].

XCAS와 유사한 아이디어를 가지고 등장한 제품은 미국 케이블통신협회(NCTA, The National Cable & Telecommunications Association)에서 차세대 네트워크 아키텍처(NGNA, Next Generation Network Architecture)의 일환으로 개발한 DCAS(Downloadable CAS)가 있다. NGNA는 미국 3대 MSO인 컴캐스트, 콕스 커뮤니케이션, 타임워너 케이블이 주축이 되어있으며 현재 케이블 TV망인 광동축 혼합망(HFC, Hybrid Fiber Coax) 인프라에 추가적인 비용 투자 없이 제품혁신과 가격절감을 유도하는 통합 멀티미디어 구조의 구현을 목표로 하고 있다. NGNA에서는 소프트웨어 다운로딩 방식을 도입한 NGNA 보안 모델이 있는데, 기존 디지털 방송의 보안 모델과 뚜렷한 차이점은 하드웨어



(그림 1) XCAS 구조[2]

기반 시스템을 원격으로 재구성할 수 있고, 소프트웨어 기반 시스템도 다운로드에 의해 접근제어시스템의 일부를 업데이트 할 수 있다는 점이다. NGNA의 보안 모델은 크게 3가지 서브 시스템으로 구성된다[1-4, 19].

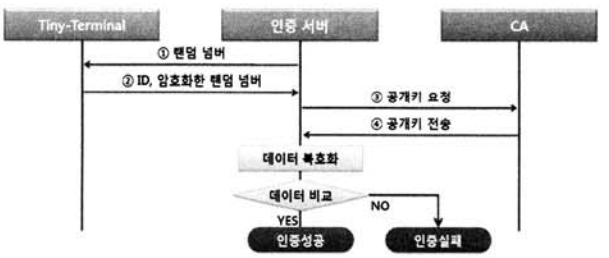
- 하드웨어 기반이나 원격으로 재구성 가능한 콘텐트와 키 암호화/복호화 시스템
- 소프트웨어 기반 접근제어 모듈의 다운로딩으로 재정의 할 수 있는 키 관리 시스템
- 부분적인 소프트웨어 기반 접근제어 모듈 다운로딩으로 업데이트 가능한 인증 시스템

미국의 MSO들은 연방통신위원회가 규정하고 있는 분리의무화를 케이블카드를 교체하는 셋탑 박스 뿐만 아니라 소프트웨어 다운로딩 방식의 XCAS까지 포함하도록 요구하고 있다. 이와 같이 XCAS는 점차 기존의 수신제한시스템을 대체하여 케이블 및 위성방송 시스템과 같은 유료시스템의 대표적인 수신제한시스템으로 자리를 잡아가고 있다[1-4, 19].

2.2 공개키 기반 장치 인증에 대한 논문과 특허에 대한 분석

현재 XCAS에서 셋탑 박스를 인증하기 위해 사용되고 있거나 제안되어 있는 장치 인증 방법은 존재하지 않는다. 따라서 본 논문에서는 타 환경에서 제안된 장치 인증 방법들을 분석하여 그 결과를 바탕으로 XCAS에서의 셋탑 박스 인증 방법을 제안 하고자 한다.

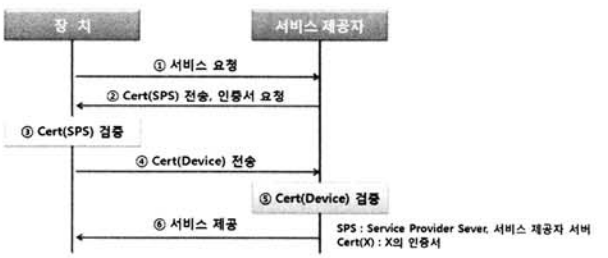
Park 등은 유비쿼터스 컴퓨팅 환경에서 상호 운영성 및 확장 가능성을 가진 PKI를 사용한 상호 인증 시스템을 제안한다. 해당 논문에서 제안하는 개선된 인증 시스템을 Tiny-Terminal 시스템이라 하며, 이는 싱글 사인온(SSO, Single Sign-On) 방식을 추구한다. 본 논문에서 제안하는 스킴은 Tiny-Terminal, 인증서버, 인증기관(CA, Certificate Authority)로 구성된다[5]. 해당 논문에서 제안하는 인증 방식은 (그림 2)와 같다.



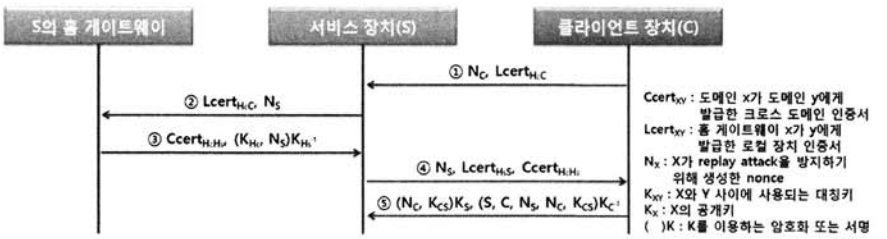
(그림 2) Park 등의 인증기법[5]

Hwang 등은 다중도메인(Multi-Domain)을 가지는 홈 네트워크 환경에서 PKI를 이용한 장치 인증을 제안한다. 해당 논문에서는 효율성 제고를 위해 PKI를 Global PKI 계층, Localized PKI 계층 두 개의 계층으로 나누어 장치 인증을 수행한다. 현재 널리 쓰이고 있는 PKI 방식을 Global PKI 계층라고 하며, 홈 네트워크를 하나의 도메인으로 간주하여 해당 도메인 내에서 PKI를 응용한 방식을 Localized PKI 계층라고 한다. 이러한 계층 분리를 통해 Global PKI 계층에서는 도메인을 인증하는 역할을 수행하고, Localized PKI 계층에서는 각각의 장치에 대한 인증만을 담당하게 된다. 더불어 Global PKI에서는 각각의 도메인을 인증하는 역할을 수행하기 때문에 서로 다른 도메인에 대한 인증이 CA를 통해 이루어질 수 있다. 또한 CA로부터 신뢰된 도메인 내에서의 장치 인증 및 통신이 이루어질 수 있다. 이러한 방식을 통하여 현재 사용되고 있는 PKI와 경량화된 PKI를 동시에 사용하여 장치의 부담을 경감시키고자 하였다. 해당 논문에서는 인증서 발급 절차(장치 등록 과정), 도메인 내 장치 인증 절차, 도메인 간 인증 절차, 도메인 간 장치 인증 절차를 제안하고 있다[6]. 해당 논문에서 제안하는 도메인 간 장치 인증 절차는 (그림 3)과 같다.

Lee 등은 홈 네트워크 환경에서 PKI를 기반으로 하는 장치 인증 방법을 제안한다. 해당 논문에서 제안하는 인증 체계는 Root CA와 하부 CA, 각 홈 내에서 RA 역할을 하는 HRA(Home Registration Authority)와 실제 인증을 해야 하는 홈 장치들로 이루어져 있다. 이때 사용되는 인증서는 X.509를 기반으로 하며 HRA Information, HRA Ownership, Device Description 등의 확장 필드가 포함된다. 해당 논문에서는 장치 인증서 발급 방법, 콘텐츠 공유 등을 위한 홈 내의 장치 인증 방법, 서비스 제공자와 장치 인증 방법, 인증서를 이용한 분실 장치 추적 방법 등을 제안하고 있다[18]. 해당 논문에서 제안하는 서비스 제공자와 장치 인증 방법은 (그림 4)와 같다.



(그림 4) Lee 등의 인증기법[18]



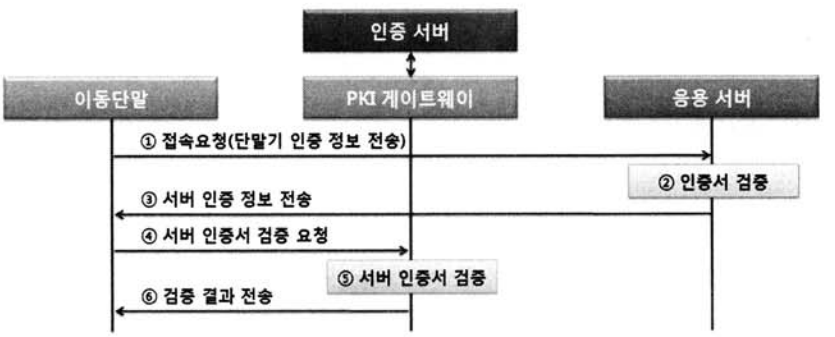
(그림 3) Hwang 등의 인증기법[8]

주식회사 데이콤의 인증기법은 마이크로 익스플로워가 탑재된 이동 단말을 이용하여 인터넷 상의 응용서버와 인증을 수행하기 위한 방법에 관한 것이다. 해당 특허에서 발명한 인증 시스템 및 방법은 공개키를 기반으로 하며 능력이 상대적으로 열악한 무선 웹 환경에서의 장치 인증을 위한 것이다. 발명한 인증 방법은 PKI 게이트웨이를 별도로 두어 모바일 기기의 인증부담을 경감하고 있다[7]. 해당 특허에서 제안하는 인증 방식은 (그림 5)와 같다.

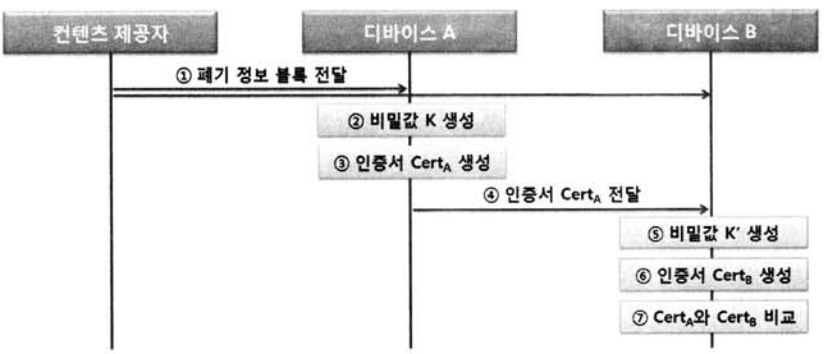
삼성전자주식회사의 인증기법(1)은 인증서를 이용한 디지털 컨텐츠 처리기기 간의 인증에 관한 내용으로 홈 네트워크에서 공개키 인증서를 이용하여 인증을 수행하는 디지털 컨텐츠 처리기기에 관한 발명이다. 발명한 인증 방법은 각 장치마다 비밀키를 저장하고 있으며, 해당 비밀키와 인증서를 사용하여 장치 인증 수행한다[8]. 해당 특허에서 제안하는 인증 방식은 (그림 6)과 같다.

한국전자통신연구원의 인증기법은 기존 PKI 인프라가 없는 P2P(Peer-to-Peer) 네트워크 환경에서 PKI 기반 구조를 활용한 인증 기법을 적용하여 안전하게 공개키의 소유권을 인증할 수 있는 방법 및 장치를 제공하는 것이 목적이다. 해당 특허는 PKI 기반 구조를 활용한 인증 기법을 적용하기 위하여 피어간 키를 생성, 전달, 검증하는 방법에 관련된 발명으로 P2P 환경을 도메인별로 나누어 해당 도메인 내에 존재하는 피어들 간의 인증방법 기술한다[9]. 해당 특허에서 제안하는 인증 방식은 (그림 7)과 같다.

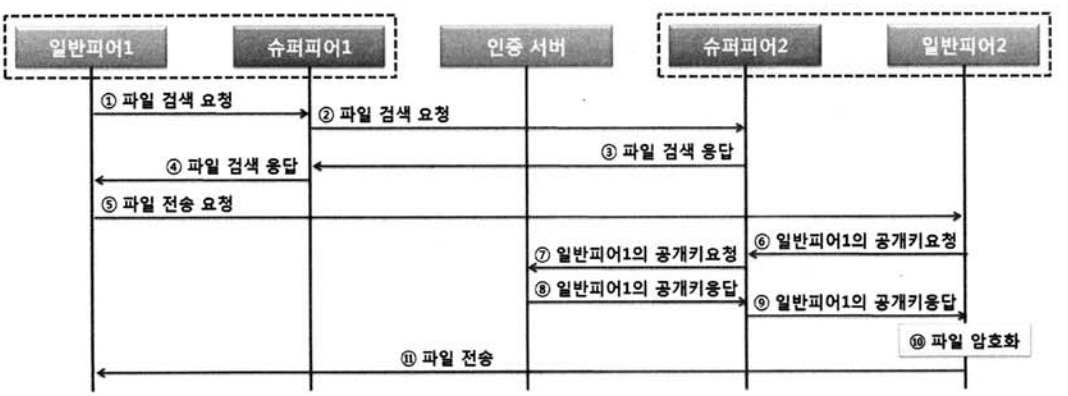
삼성전자주식회사의 인증기법(2)은 이동 통신망 환경에서 단말이 보안서비스를 받기 위한 인증 방법에 관한 내용이



(그림 5) 주식회사 데이콤의 인증기법[7]



(그림 6) 삼성전자주식회사의 인증기법(1)[8]

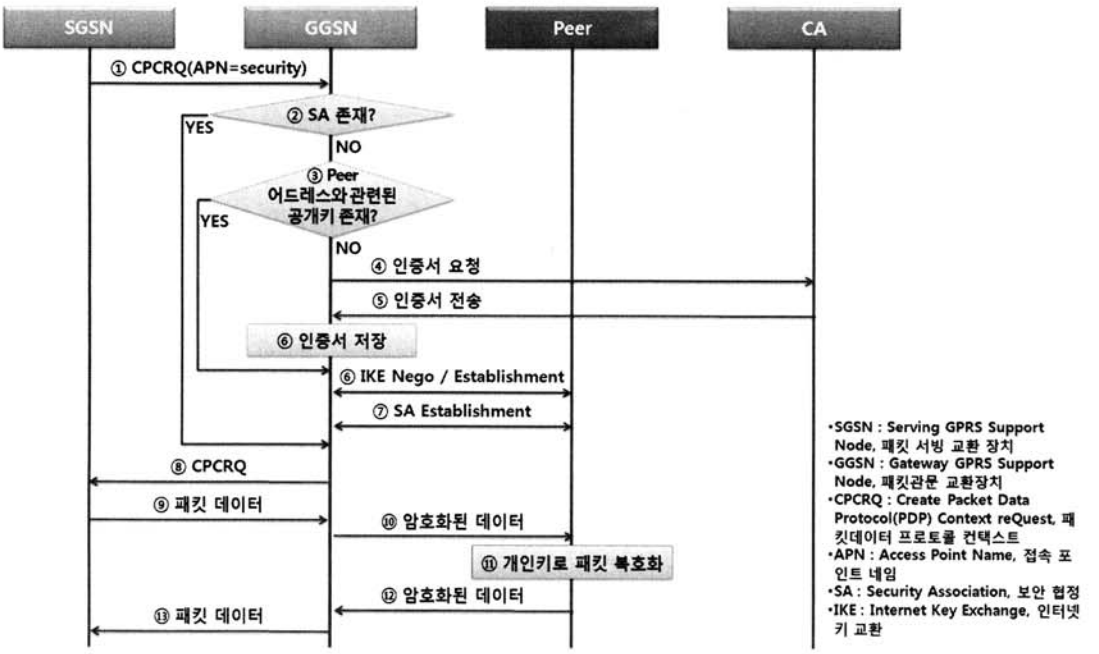


(그림 7) 한국전자통신연구원의 인증기법[9]

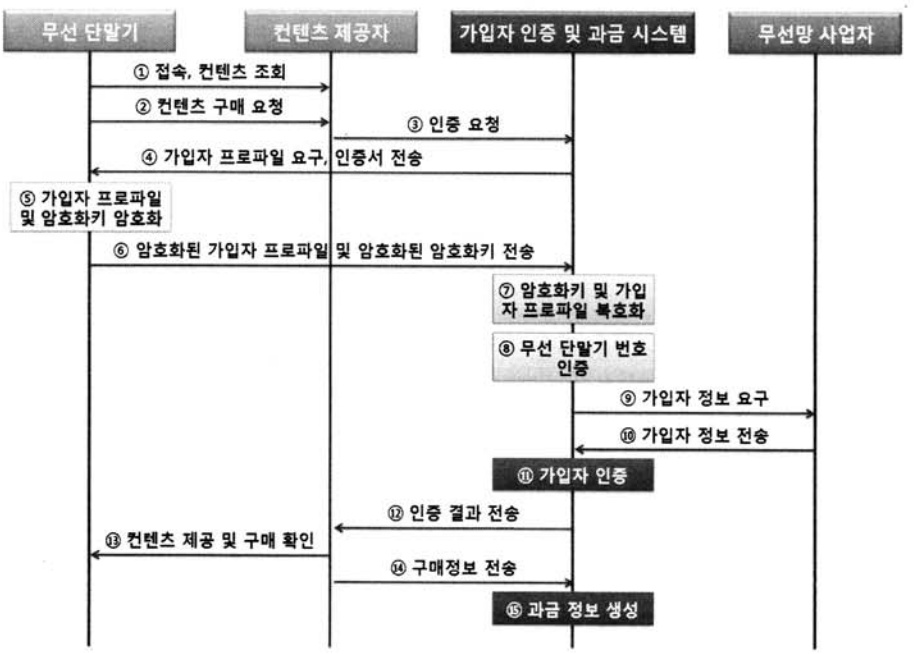
다. 해당 특허에서는 단말이 보안 서비스를 받고자 할 때 보안 게이트웨이와 상대 노드간에 보안 키 교환(IKE, Internet Key Exchange) 절차 시, 공개키를 얻어 오기위해 공개키 기반구조를 사용하는 방법 및 장치를 제공한다[10]. 해당 특허에서 제안하는 인증 방식은 (그림 8)과 같다.

에스케이텔레콤주식회사의 인증기법은 무선 단말기 가입자가 속한 무선 통신망을 포함하는 유선 통신망 및 가입자가 속해있지 않은 타 무선 통신망을 포함하는 유선 통신망에서 무선 통신 단말기의 인증/과금 시스템 및 방법에 대한 발명이다. 유무선 통신 구간에서 무선 단말 가입자 프로파일을 암호화하여 전송함으로써 가입자 프로파일의 변조/오용의 방지를 목표로 한다[11]. 해당 특허에서 제안하는 인증 방식은 (그림 9)와 같다.

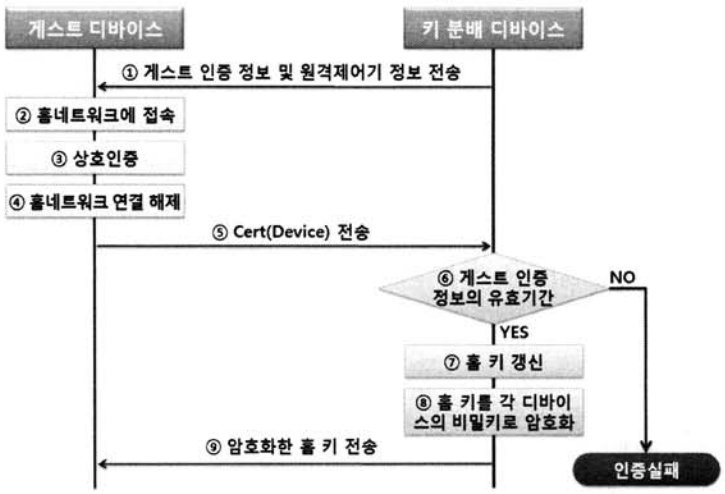
주식회사 한마로의 인증기법은 인증서를 기반으로 디지털 콘텐츠를 인증하고 그 처리를 제어하는 시스템에 관한 것으로 모바일 콘텐츠의 상호 운용성 또는 호환성을 확보하면서도 콘텐츠에 대한 보안성을 강화하는 것을 목적으로 한다[12]. 해당 특허에서 제안하는 인증 방식은 (그림 10)과 같다.



(그림 8) 삼성전자주식회사의 인증기법(2)[10]



(그림 9) 에스케이텔레콤주식회사의 인증기법[11]



(그림 10) 주식회사 한마로의 인증기법[12]

3. XCAS에 적합한 PKI기반의 장치 인증 제안

3.1 XCAS 장치 인증에서 고려되어야 하는 요구사항

3.1.1 XCAS 인증 고려사항

XCAS에서는 기존의 방송 시스템보다 가입자의 방송 사업자간 이동이 더욱 간편해진다. 따라서 방송 사업자의 가입자 변화가 커질 것으로 예상되며, 그에 따라 인증 시스템에서 추가되거나 제거되는 셋탑 박스도 많을 것이다. 그런데 대칭키 기반의 인증 방식을 사용 할 경우 새로운 장치가 추가되거나 제거될 때마다 사전에 비밀키를 공유/폐기하거나, 키분배 과정이 이루어 져야 한다. 따라서 대칭키 인증 방식 보다는, 공개키 기반 인증 방식이 XCAS 장치 인증 시스템에 적합하다.

이 때 모든 방송사업자의 인증서를 해당 셋탑 박스가 저장하고 관리하는 것은 셋탑 박스뿐만 아니라 CA에도 큰 부담이 될 수 있다. 또한 일반 컴퓨터보다 상대적으로 약한 XCAS 셋탑 박스의 저장 및 연산 능력 등을 고려하여 해당 셋탑 박스가 저장하고 관리하는 인증서의 개수를 최소화 하는 것이 바람직하다. 해당 셋탑 박스 인증 절차도 기존 PKI를 활용할 수 있도록 호환성을 유지하는 방안이 요구되며, 해당 PKI 기반 인증서가 활용되는 환경에 적합한 키 길이, 인증서 유효기간을 지정하여 인증 절차가 안전하게 이루어질 수 있도록 보장해야 한다.

또한, 기존의 공인인증서는 인터넷 뱅킹, 전자 결제 등에 사용되어 CA와 등록대행기관(RA, Registration Authority)이 현재의 공인인증서 체계에 맞게 구성되어 있으므로 이와는 별도로 셋탑 박스 인증 절차에 참여하는 주체들이 적절한 역할을 수행하고 방송 서비스용 인증서를 관리하기에 적합한 CA와 RA의 제안이 필요하다.

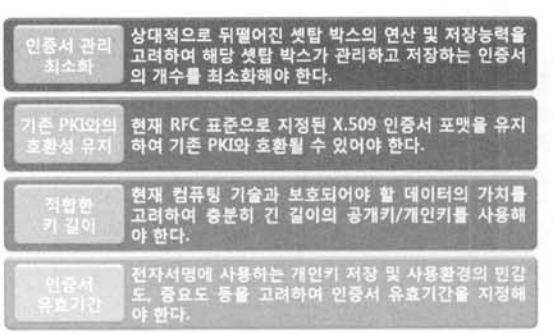
3.1.2 XCAS 인증 보안 요구사항

XCAS 셋탑 박스 인증 시에 가능한 공격 방법은 다음과 같다.

· 재사용 공격(Replay attack)
공격자가 합법적인 사용자로 위장하거나 정당한 사용자와 세션키를 설정하기 위해 이전 프로토콜에서 사용된 메시지를 재사용하는 공격을 말한다. Replay attack에는 송신자의 메시지가 송신자에게 다시 되돌아가는 reflection attack과 제 3자에게 재사용되는 interleaving attack이 있다. 시점확인, 연속된 수, 난수 등의 매개변수를 검증자의 응답 메시지에 추가함으로써 한번 사용한 응답 메시지는 더 이상 사용할 수 없도록 함으로써 이 공격을 방지할 수 있다.[20, 27]

· Unknown key-share
이 공격은 실제 A와 B가 통신하고 있는 상황에서 A는 B와 B는 A가 아닌 C와 공통 키를 나누어 가졌다고 생각하게 만드는 공격을 말한다. 공격자가 프로토콜 진행 중에 전송되는 정보를 지연시킨 후 온라인으로 인증서를 발급해주는 CA로 부터 공개키 인증서를 받을 수 있다면 가능하다.[21]

· Small subgroup attack
Small subgroup attack은 Diffie-Hellman(DH) 기반의 키 동의 프로토콜에서 g의 위수(order)가 합성수일 경우, g는 부분군(subgroup)을 가지게 된다는 점을 이용하여 공격자가 DH기반의 프로토콜에서 생성되는 세션키에 대한 전수조사(Brute Force Attack) 시 mod p상의



(그림 11) 요구사항

모든 값을 대입하지 않고, 부분군(subgroup)내의 모든 수만을 대입하는 공격이다. g를 선택할 때, 위수가 p-1의 약수이면서 소수인 위수를 선택하면 대응 가능 하다.[22]

- Parsing Ambiguity

Parsing Ambiguity는 2008년 Liqun Chen, Chris J. Mitchell의 "Parsing ambuities in authentication and key establishment protocols"에 의해 알려진 메시지 파싱 과정에서의 모호함을 이용하는 공격이다. Parsing ambiguous attack은 기존에 사용된 메시지 없이도 프로토콜 자체만으로 공격이 가능하며, 국제표준(ISO/IEC)에 명세된 대부분의 프로토콜에 적용 가능하다. 이 공격은 메시지 필드의 비트 길이 수를 명시하면 대응 가능하다.[23]

- 중간자 공격(Man-in-the-middle attack)

중간자 공격(Man-in-the-middle attack)은 인터넷 이용자의 정보 및 자원에 대한 통제권을 획득하기 위해 공격자가 사용자와 대상의 중간에 자신의 사이트를 위치하여 커뮤니케이션의 조정자 역할을 수행하면서 모든 메시지를 수집 및 관찰하는 공격이다. 피싱(Phishing) 또는 파밍(Pharming) 형태로 구현된다.[24]

- Parallel Session Attack

Parallel Session Attack은 공격자가 공격 대상자 B와 2개 이상의 연결 채널을 형성하여, 이전 채널에서 사용한 정보를 다른 채널에서 적용하는 공격이다. 공격자는 시스템 내의 정상적인 사용자 A로 위장하여 다른 채널을 형성하고, 공격에 성공하면 B는 공격자가 아닌 A와 통신하는 것으로 인식하게 된다.[25]

- Modification Attack

Modification Attack은 공격자가 정상적인 사용자 A, B가 통신하고 있을 때, 이들 간의 메시지를 수정하여 잘못된 키를 맺도록 유도하거나 인증 값을 알아내는 공격이다. 공격자는 정상적인 사용자 A와 통신할 때 자신의 메시지를 수정하여 인증이 성공하도록 유도하거나, 상대방의 인증 값을 알아낸다.[26]

3.2 제안하는 셋탑 박스 인증 체계

국내 유료 방송 서비스 가입 가구수는 약 1700만 가구이다[13]. 따라서 인증서를 기반으로 하는 셋탑 박스 인증 체계는 2000년~2007년에 발행된 개인용 공인인증서가 약 1600만 건인 것을 감안할 때 국내 민간 공인인증체계와 유사한 규모가 된다[14]. 따라서, 셋탑 박스 인증을 위한 새로운 체계를 구축하는 것보다 공인인증체계를 이용하는 것이 합리적이다. 제안하는 셋탑 박스 인증 체계는 (그림 12)와 같다.

〈표 1〉 셋탑 박스 인증 체계 요소와 선정 근거

구분	제안
Root CA	민간 최상위 인증기관
CA_1, CA_2, …, CA_5	기존 공인인증 시스템의 CA
CA_6	국가에서 인정하는 디지털케이블TV의 방송·통신에 관한 기술 표준 및 인증 기관

국내 공인인증서 기반을 이용하며 방송 서비스용 인증 시스템에 사용될 특수 목적의 공인인증서를 발급하는 6번째 CA를 지정한다. CA_6은 하위에 MSO와 MNF(Manufacture)를 가지고 있다.

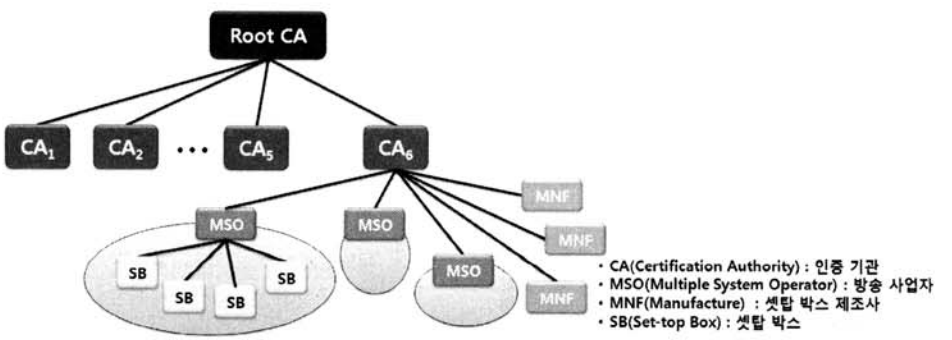
6번째 CA는 국가에서 인정하는 방송·통신 융합의 핵심 매체인 디지털케이블TV의 방송·통신에 관한 기술 표준 및 인증과 관련된 업무를 수행하는 기관이어야 한다. 6번째 CA는 MSO와 MNF를 선정하고 인증서를 발급하며 주기적으로 현재 인증 받은 MNF 목록을 MSO로 브로드캐스팅 해주어야 한다. 이러한 과정 중 각종 법·제도나 기술 규격은 공인인증서와 동일하게 적용해야하며 OCSP(Online Certificate Status Protocol) 서버 등 인증서 관리와 관련된 각종 시스템은 기존 공인인증 체계에 구축되어 있는 것을 활용할 수 있다.

MNF는 셋탑 박스 제조사로 6번째 CA의 인증을 받은 업체이다. MNF는 셋탑 박스 인증서에 대한 RA라고 할 수 있으며 자신이 제작하는 모든 셋탑 박스에 대해 셋탑 박스 인증서를 발행하여 저장해야 한다.

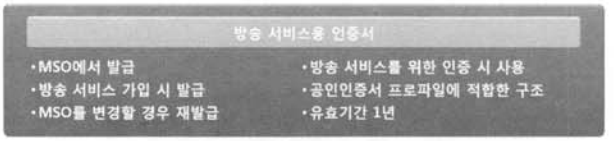
MSO는 6번째 CA의 인증을 받은 방송 사업자로 방송 서비스용 인증서에 대한 RA라고 할 수 있다. MSO는 셋탑 박스에 방송 서비스용 인증서를 발급한다. 또한 서비스 가입 SB(Set-top Box) 목록을 유지 및 검증할 수 있는 시스템을 구축해야 한다.

3.3 제안하는 인증서 구조

제안하는 인증 체계에서 사용되는 인증서는 두 가지 이다. 하나는 MSO에서 셋탑 박스에 발급하는 방송 서비스용



(그림 12) 셋탑 박스 인증 체계



(그림 13) 방송 서비스용 인증서

인증서이고 두 번째는 MNF에서 제조시 셋탑 박스에 저장하는 셋탑 박스 인증서이다. 셋탑 박스 인증서는 방송 서비스용 인증서 발급 시에 사용된다.

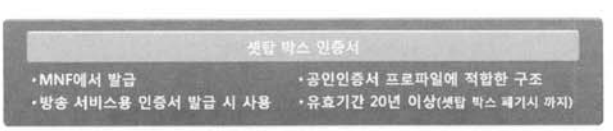
방송 서비스용 인증서는 MSO에서 방송 서비스를 요청하는 셋탑 박스로 발급하며 방송 서비스를 위한 셋탑 박스 인증 시에 사용된다. 동일한 방송 서비스를 이용하는 도중에 인증서 유효기간이 만료될 경우 해당 MSO를 통해 인증서를 갱신하며, 다른 방송 서비스를 이용 할 경우 사용하고 있던 방송 서비스용 인증서를 폐기한 후 새로운 MSO에서 재발급 받는다. 제안하는 방송 서비스용 인증서는 (그림 13)과 같다.

인증서에 사용되는 알고리즘은 셋탑 박스의 계산 능력을 고려하여 공개키 알고리즘 중 가능한 알고리즘을 선택하여 사용하면 된다. 또한 셋탑 박스의 계산 능력과 관련하여 셋탑 박스의 전원을 켤 때 마다 MSO와 인증하는데 무리가 없는 정도의 키 길이를 가질 수 있어야 한다. 그러므로 방송 서비스용 인증서의 유효기간은 안전성에 무리가 없는 정도 하에서 충분히 짧아야 한다. NIST SP 800-57 Part1 (National Institute of Standards and Technology, Special Publication 800-57 Part1)에서는 서명에 사용되는 개인키는 민감도, 중요도 등을 고려하여 1년에서 최대한 3년을 주기로 폐기하고 새로 생성하도록 권고한다[15]. 또한 현재 국내 개인 가입자용 공인인증서 유효기간은 1년이다. 그러므로 방송 서비스용 인증서 유효기간은 1년으로 하는 것이 적합하다.

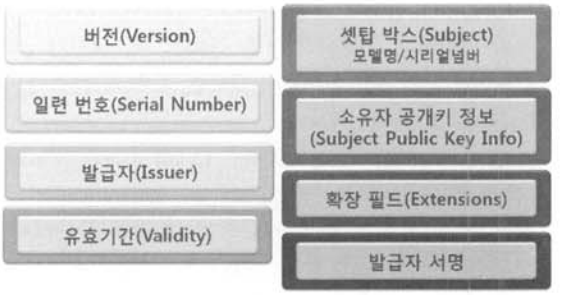
셋탑 박스 인증서는 셋탑 박스 폐기 시까지 사용 할 수 있는 긴 유효기간을 가져야 하고 MNF에서 셋탑 박스에 저장한 이후에는 갱신되거나 폐기되지 않는다. 셋탑 박스가 MSO에서 방송 서비스용 인증서를 발급 받을 때 사용한다. 제안하는 셋탑 박스 인증서는 (그림 14)와 같다.

셋탑 박스 인증서는 셋탑 박스 제조 시에 MNF에서 발급하여 셋탑 박스에 저장한다. 따라서 셋탑 박스 사용자는 직접 셋탑 박스 인증서를 갱신할 수 없다. 따라서 한번 발급 받은 셋탑 박스 인증서는 셋탑 박스를 폐기할 때까지 사용해야 한다.

NIST가 권고하는 서명용 키 사용기간은 최대 3년이나, 공인인증업무준칙에 따르면 공인인증 기관의 인증서 유효기간은 10년 이내로 설정하는 것이 가능하며, 특히 인터넷진흥원의 공인인증서의 유효기간은 20년 이내까지 가능하다 [16]. 이러한 사실을 고려하여 적절한 키 길이를 설정하여 셋탑 박스 사용 가능 기간과 유사한 길이의 셋탑 박스 유효



(그림 14) 셋탑 박스 인증서



(그림 15) 셋탑 박스 인증서 필드

기간을 설정해야 한다.

현재는 수신제한시스템을 사용하고 있기 때문에 MSO를 옮길 때마다 셋탑 박스를 교체하여 평균 셋탑 박스 사용기간에 대한 통계가 없다. 그러나 셋탑 박스와 밀접한 관계가 있는 가전제품인 TV의 경우 약 10년의 주기로 교체 한다는 것을 알 수 있다[17]. 따라서 셋탑 박스의 사용 가능 기간 역시 약 10년 정도라고 가정 하면, 2048 bits 이상의 키 길이를 사용할 때 약 10년의 유효기간을 가지는 인증서를 사용 할 수 있다.

제안하는 방송 서비스용 인증서와 셋탑 박스 인증서의 필드 구성은 공인인증서 프로파일에 적합한 구조를 가진다. 따라서 제안 하는 인증서의 기본 필드 구성은 (그림 15)와 같다.

일반적으로 '소유자'라고 부르는 Subject 필드에는 해당 셋탑 박스에 대한 정보가 들어가게 된다. 이때 셋탑 박스의 정보는 모델명과 시리얼 넘버가 필수적으로 포함 되어야 한다. 인증서 필드 중 발급자(Issuer)는 방송 서비스용 인증서의 경우 MSO, 셋탑 박스 인증서의 경우 MNF를 의미하며, 위의 인증서에 포함 되는 모든 정보는 발급자(Issuer)에 의해 서명된다. 추가적인 셋탑 박스 정보 등 기타 필요하다고 판단되는 항목은 확장필드에 추가 할 수 있다.

3.4 제안하는 방송 서비스용 인증서 발급 절차

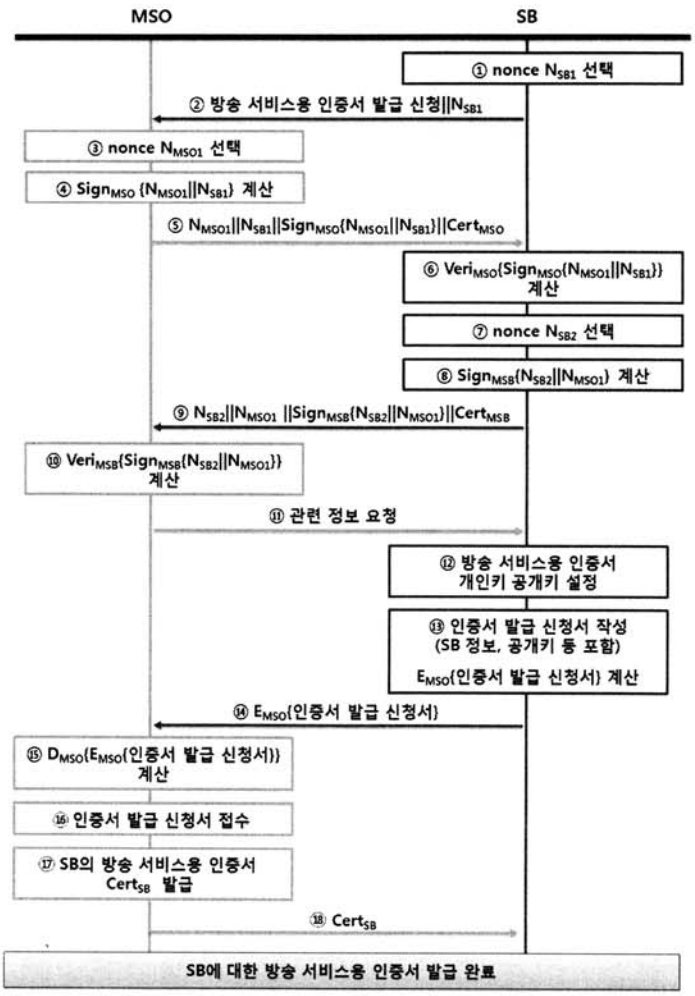
셋탑 박스가 MSO에게 방송 서비스용 인증서를 발급받는 절차는 크게 셋탑 박스 검증, 개인키/공개키 계산, 인증서 발급의 세단계로 이루어진다. 첫 번째 단계인 셋탑 박스 검증시에 MNF에서 셋탑 박스 제조시 저장한 셋탑 박스 인증서를 사용한다. 제안 하는 방송 서비스용 인증서 절차는 (그림 16)과 같다.

① 셋탑 박스는 nonce N_{SB1}을 선택한다. 단, 셋탑 박스에서 nonce를 생성하는 의사난수함수(PRF, Pseudo Random Number Function)는 충분히 랜덤성을 갖는 nonce를 생성한다고 가정한다.

② 셋탑 박스는 MSO에게 방송 서비스용 인증서 발급 요청을 한다.

③ MSO는 nonce N_{MSO1}을 선택한다. 단, MSO에서 nonce를 생성하는 의사난수함수는 충분히 랜덤성을 갖는 nonce를 생성한다고 가정한다.

④ MSO는 $N_{MSO1}||N_{SB1}$에 서명한다.



(그림 16) 방송 서비스용 인증서 발급 절차

⑤ MSO는 $N_{MSO1}||N_{SB1}$, $N_{MSO1}||N_{SB1}$에 서명한 값 $Sign_{MSO}\{N_{MSO1}||N_{SB1}\}$, 자신의 인증서($Cert_{MSO}$)를 셋탑 박스에게 전송한다.

⑥ 셋탑 박스는 $Sign_{MSO}\{N_{MSO1}||N_{SB1}\}$을 검증한다. 검증에 성공한다면 다음단계로 계속 진행하고, 검증에 실패한다면 새로운 nonce N_{SB1}'을 선택하고 MSO에게 다시 방송 서비스용 인증서 발급 요청을 한다.

〈표 2〉 방송 서비스용 인증서 발급 절차 표기법

MSO	방송 사업자
SB	셋탑 박스
$Cert_{MSO}$	6번째 CA에서 인증한 MSO의 인증서
$Cert_{MSB}$	SB의 셋탑 박스 인증서
$Cert_{SB}$	SB의 방송 서비스용 인증서
$Sign_{MSO}\{\ \}$	MSO의 서명 함수
$Veri_{MSO}\{\ \}$	MSO의 검증 함수
$Sign_{MSB}\{\ \}$	SB의 셋탑 박스 인증서를 이용하는 서명 함수
$Veri_{MSB}\{\ \}$	SB의 셋탑 박스 인증서를 이용하는 검증 함수
$E_{MSO}\{\ \}$	MSO의 암호화 함수
$D_{MSO}\{\ \}$	MSO의 복호화 함수

⑦ 셋탑 박스는 nonce N_{SB2}를 선택한다.

⑧ 셋탑 박스는 $N_{SB2}||N_{MSO1}$에 셋탑 박스 인증서로 서명한다.

⑨ 셋탑 박스는 $N_{SB2}||N_{MSO1}$, $N_{SB2}||N_{MSO1}$에 서명한 값 $Sign_{MSB}\{N_{SB2}||N_{MSO1}\}$, 자신의 셋탑 박스 인증서($Cert_{MSB}$)를 셋탑 박스에게 전송한다.

⑩ MSO는 $Sign_{MSB}\{N_{SB2}||N_{MSO1}\}$을 검증한다. 검증에 성공한다면 다음단계로 계속 진행되고, 검증에 실패한다면 셋탑 박스로 인증서 발급 거부 메시지를 전송한 후 종료한다.

⑪ MSO는 셋탑 박스에서 인증서를 발급 하는데 필요한 정보를 요청한다.

⑫ 셋탑 박스는 방송 서비스용 인증서에 필요한 개인키와 공개키를 생성한다.

⑬ 셋탑 박스는 셋탑 박스 정보, 공개키 등이 기록된 인증서 발급 신청서를 작성하고 작성된 인증서 발급 신청서를 MSO의 공개키로 암호화 한다. 인증서 발급 신청시 필요한 항목은 (그림 17)과 같다.

⑭ 셋탑 박스는 암호화된 인증서 발급 신청서를 MSO로 전송한다.

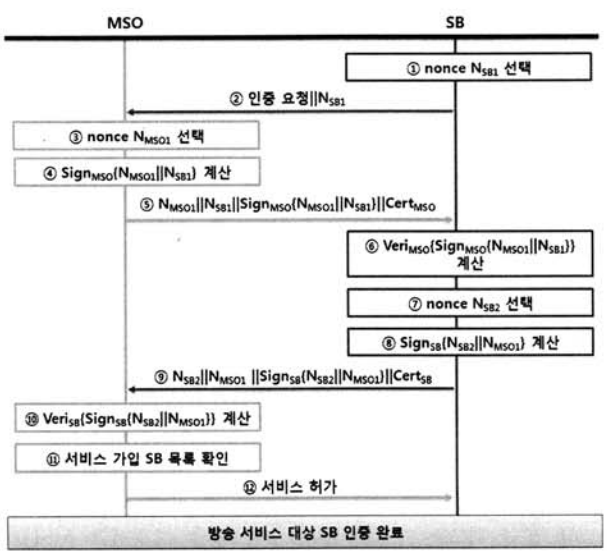
(그림 17) 인증서 발급 신청서 필드

⑮ MSO는 E_{MSO}{인증서 발급 신청서}를 복호한다.
⑯ MSO는 인증서 발급 신청서의 내용을 확인한 후 인증서 발급 신청을 접수한다.
⑰ MSO는 셋탑 박스의 방송 서비스용 인증서 $Cert_{SB}$를 발급한다.
⑱ MSO는 발급한 셋탑 박스의 방송 서비스용 인증서 $Cert_{SB}$를 셋탑 박스에게 전송한다.

3.5 셋탑 박스 인증 절차

제안 하는 셋탑 박스 인증 절차는 (그림 18)과 같다.

① 셋탑 박스는 nonce N_{SB1}을 선택한다. 단, 셋탑 박스에서 nonce를 생성하는 의사난수함수는 충분히 랜덤성을 갖는 nonce를 생성한다고 가정한다.
② 셋탑 박스는 MSO에게 인증 요청을 한다.
③ MSO는 nonce N_{MSO1}을 선택한다. 단, MSO에서 nonce를 생성하는 의사난수함수는 충분히 랜덤성을 갖는 nonce를 생성한다고 가정한다.
④ MSO는 $N_{MSO1}||N_{SB1}$에 서명한다.
⑤ MSO는 $N_{MSO1}||N_{SB1}$, $N_{MSO1}||N_{SB1}$에 서명한 값 $Sign_{MSO}\{N_{MSO1}||N_{SB1}\}$, 자신의 인증서($Cert_{MSO}$)를 셋탑 박스에게 전송한다.
⑥ 셋탑 박스는 $Sign_{MSO}\{N_{MSO1}||N_{SB1}\}$을 검증한다. 검증에 성공한다면 다음단계로 계속 진행하고, 검증에 실패한다면 새로운 nonce N_{SB1}'을 선택하고 MSO에게 새로운 인증 요청을 한다.
⑦ 셋탑 박스는 nonce N_{SB2}를 선택한다.
⑧ 셋탑 박스는 $N_{SB2}||N_{MSO1}$에 방송 서비스용 인증서로 서명한다.
⑨ 셋탑 박스는 $N_{SB2}||N_{MSO1}$, $N_{SB2}||N_{MSO1}$에 서명한 값 $Sign_{SB}\{N_{SB2}||N_{MSO1}\}$, 자신의 방송 서비스용 인증서($Cert_{SB}$)를 셋탑 박스에게 전송한다.
⑩ MSO는 $Sign_{SB}\{N_{SB2}||N_{MSO1}\}$을 검증한다. 검증에 성공한다면 다음단계로 계속 진행되고, 검증에 실패한다면 셋탑 박스로 인증서 발급 거부 메시지를 전송한 후 종료한다.
⑪ MSO는 $Cert_{SB}$의 셋탑 박스가 서비스 가입 SB 목록에 기재되어 있는지 확인한다. 목록 기재되어 있지 않다면 셋탑 박스로 서비스 거부 메시지를 전송한 후 종료하고, 기재되어 있다면 다음단계로 계속 진행한다.
⑫ MSO는 서비스 허가 메시지를 보낸 뒤 서비스를 시작한다.



(그림 18) 인증 절차

〈표 3〉 인증 절차 표기법

MSO	방송 사업자
SB	셋탑 박스
$Sign_{MSO}\{\ \}$	MSO의 서명 함수
$Veri_{MSO}\{\ \}$	MSO의 검증 함수
$Cert_{MSO}$	6번째 CA에서 인증한 MSO의 인증서
$Cert_{SB}$	SB의 방송 서비스용 인증서
$Sign_{SB}\{\ \}$	SB의 방송 서비스용 인증서를 이용하는 서명 함수
$Veri_{SB}\{\ \}$	SB의 방송 서비스용 인증서를 이용하는 검증 함수

4. 제안한 인증 절차의 효율성 및 안전성

제안한 셋탑 박스 인증 체계에 대한 효율성과 안전성 분석을 수행한다. 셋탑 박스 인증 절차는 크게 (1) 셋탑 박스 인증서 발급, (2) 방송 서비스용 인증서 발급, (3) 셋탑 박스 인증 세단계로 구성되어 있다. 이중 셋탑 박스 인증서 발급은 제조사에서 셋탑 박스 제조시에 이루어지고, 방송 서비스용 인증서 발급 절차와 셋탑 박스 인증 절차는 유사하므로 셋탑 박스 인증 절차에 대한 분석만 수행한다.

4.1 효율성

제안한 셋탑 박스 인증 절차의 효율성 분석은 2장에서 분석한 장치 인증에 대한 특허 및 논문과 비교를 통해 알 수 있다. 제안한 셋탑 박스 인증 절차와 분석된 특허/논문의 효율성을 비교한 결과는 <표 4>와 같다.

효율성을 측정 하는 요소는 서명 및 검증 횟수, 암호화 및 복호화 횟수, 데이터 전송 횟수, 주체 수로 선정 하였다. 비교 결과에 따르면 제안한 셋탑 박스 인증 절차는 서명 및 검증 횟수가 비교적 많은 편이지만, 암호화 및 복호화 과정이 없고 데이터 전송 횟수 및 인증에 관여하는 주체 수가 현격히 적다. 따라서 인증과정의 전체적인 효율성이 뛰어나다.

〈표 4〉 제안한 인증 절차와 분석 특허/논문 효율성 비교

구 분	서명 및 검증	암호화 및 복호화	데이터 전송 횟수	주체 수
Park 등의 인증기법	2	0	4	3
Hwang 등의 인증기법 ※	2 이상	1 이상	5 이상	5
Lee 등의 인증기법 ※	2 이상	0	4 이상	4
주식회사 데이콤의 인증기법	4	0	4	4
삼성전자주식회사의 인증기법(1)	4	0	3	3
한국전자통신연구원의 인증기법	2	0	10	5
삼성전자주식회사의 인증기법(2)	2	4	10	3
에스케이텔레콤주식회사의 인증기법	2	2	10	4
주식회사 한마로의 인증기법	2	6	12	9
제안하는 방식	4	0	4	2

※ Ⅱ-2 절에서 소개한 인증 과정 외에 논문에서 제안된 전체적인 인증 과정을 고려하여 계산

4.2 안전성

본 논문에서는 제안하는 프로토콜을 정형적, 비정형적으로 안전성을 분석하였다.

4.2.1 비정형적 분석 방법

우선 비정형적인 안전성 분석은 Ⅲ장에서 제시한 적용 가능한 공격방법이 제안하는 인증 방법에 적용 가능한지 확인함으로써 분석이 가능하다. 기존의 장치 인증 기법에 각각의 공제안하는 셋탑 박스 인증 방법은 위의 9가지 공격에 대해 모두 안전한 것으로 분석되었으며, 분석 결과는 <표 5>와 같다.

<표 5>에서 공격이 성공할 가능성이 있다는 의미는 해당 인증방법에서 공격에 취약한 부분이 발견되었거나, 공격을 방지할 수 있는 요소에 대한 언급이 없다는 것을 의미한다. 예를 들어 각 주체가 주고받는 메시지 포맷이 명확히 표현되어 있지 않거나, 인증서의 포맷이나 갱신 주기 등에 대한 언급이 없는 경우가 있다.

· 재사용 공격(Replay attack)

제안하는 셋탑 박스 인증 절차는 메시지를 전송 할 때마다 셋탑 박스와 MSO가 각각 새로이 생성되는 난수를 Nonce로 이용하도록 구성되었다. 따라서 재사용 공격(Replay attack)에 안전하다.

· Unknown key-share

프로토콜은 Unknown key-share에 대해서 공격자가 CA의 서명을 위조할 수 없다는 가정 하에서 안전하다. 제안하는 셋탑 박스 인증 체계는 공인인증서 PKI를 수정하여 제안하고 있기 때문에, Root CA와 6번째 CA에 대해서 공인인증서 PKI에 적용되는 정책과 기술도 동일하게 적용되며 제안 하는 셋탑 박스 인증 체계에서 CA의 개인 키에 대한 안전성 역시 공인인증서 PKI와 동일한 수준이라고 가정할 수 있다. 그러므로 제안하는 셋탑 박스 인증 체계는 Unknown key-share에 대해서 안전하다.

· Small subgroup attack

제안하는 셋탑 박스 인증 방법에서는 공개키 알고리즘 중 어떤 것을 사용하는지에 대한 것 까지는 제안하지 않고 있다. 그러나 어떤 공개키 알고리즘을 사용하던지 g(또는 g와 같은 역할을 하는, ECC의 경우 베이스 포인트 G)를 선택할 때 위수를 조건에 적합한 충분히 큰 소수로 갖는 원소로 선택하면 Small subgroup attack에 대하여 안전하다.

· Parsing Ambiguity

제안하는 셋탑 박스 인증 절차에서 MSO와 셋탑 박스가 주고받는 메시지는 $[N_{MSO1}||N_{SB1}||Sign_{MSO}\{N_{MSO1}||N_{SB1}\}||Cert_{MSO}]$와 $[N_{SB2}||N_{MSO1}||Sign_{SB}\{N_{SB2}||N_{MSO1}\}||Cert_{SB}]$이다. 각 메시지의 항목은 MSO와 셋탑 박스가 직접 선택하거나 계산한 결과 값, 그리고 공개되어있는 인증서 정보이기 때문에 공격자가 Parsing Ambiguity를 이용하여 본 인증 과정을 공격할 수 없다.

· 중간자 공격(Man-in-the-middle attack)

제안하는 인증 절차에서는 인증서를 기반으로 상호인증을 수행하기 때문에 중간자 공격(Man-in-the-middle attack)에 대하여 안전하다.

· Parallel Session Attack

제안하는 인증 방법에서 Parallel Session Attack이 가능하려면 공격자가 셋탑 박스의 서명을 위조할 수 있어

〈표 5〉 제안한 인증 절차와 분석 특허/논문 공격 대응 비교

구 분	재사용 공격 (Replay attack)	Unknown key-share	Small subgroup attack	Parsing Ambiguity	중간자 공격 (Man-in-the-middle attack)	Parallel Session Attack	Modification Attack
Park 등의 인증기법	O	X	X	O	O	X	O
Hwang 등의 인증기법	X	X	X	O	X	X	X
Lee 등의 인증기법	O	X	X	O	X	X	O
주식회사 데이콤의 인증기법	O	O	X	O	X	X	O
삼성전자주식회사의 인증기법(1)	O	O	X	O	X	X	O
한국전자통신연구원의 인증기법	O	O	X	O	O	X	O
삼성전자주식회사의 인증기법(2)	O	O	X	O	X	X	O
에스케이텔레콤주식회사의 인증기법	O	O	X	O	X	X	O
주식회사 한마로의 인증기법	O	O	X	O	O	X	O
제안하는 방식	X	X	X	X	X	X	X

※ O : 해당 공격의 성공 가능성 존재 / X : 해당 공격의 성공 가능성 없음

야 한다. 따라서 제안하는 인증 방법은 셋탑 박스의 개인키가 안전하게 보관된다는 가정하여 Parallel Session Attack에 대해서 안전 하다.

· Modification Attack

제안하는 인증 방법에서 MSO와 셋탑 박스가 주고받는 메시지에는 서명 값이 포함되기 때문에, MSO와 셋탑 박스의 개인키가 안전하게 보관된다는 가정하여 Modification Attack에 대해서 안전 하다.

4.2.2 정형적 분석 방법

현재까지 알려진 암호프로토콜의 정형화된 분석 방법에는 BAN, GNY, CKT5, KPL, AT, VO, SVO 등이 있다. 그러나 BAN 로직 이후에 제안된 분석 방법들은 대부분 BAN 로직에 기반하고 있다. 따라서 제안한 인증절차에 대해서 BAN 로직을 이용하여 정형적 분석을 수행한다.

BAN 로직은 1989년에 발표된 암호 프로토콜의 정형화된 분석 방법으로 해당 프로토콜에 참여하는 주체와 전송되는 메시지에 대한 신뢰가 달성되는지 여부를 정형화된 언어로 표현하여 증명한다. BAN 로직은 초기 가정사항, 프로토콜의 이상화, 프로토콜의 목표설정, 프로토콜 검증 등 4단계로 이루어져 있다. BAN 로직의 기본 표기법은 <표 6>과 같다.

① 초기 가정사항(Initial Assumption)

본 연구에서 제안한 프로토콜에서의 초기 가정사항은 다음과 같다.

$$MSO \mid\equiv \overset{K_{MSO}}{\mapsto} MSO \quad (1) \qquad SB \mid\equiv \overset{K_{SB}}{\mapsto} SB \quad (2)$$

$$MSO \mid\equiv \overset{K_{SB}}{\mapsto} SB \quad (3) \qquad SB \mid\equiv \overset{K_{MSO}}{\mapsto} MSO \quad (4)$$

$$MSO \mid\equiv \#(N_{MSO1}) \quad (5) \qquad SB \mid\equiv \#(N_{SB1}) \quad (6)$$

$$SB \mid\equiv \#(N_{SB2}) \quad (7)$$

〈표 6〉 BAN 로직 표기법

P, Q	프로토콜 참여 주체
K	암호화 키
K_{PQ}	P와 Q 사이의 사전에 공유된 비밀키
K_P/K_P^{-1}	P의 공개키/개인키
P |≡ Q	P는 Q를 믿는다.
P ◁ X	P는 X를 볼 수 있다.
P |~ X	P는 X를 이전에 전송한 적이 있다.
P ⇒ X	P는 X에 대한 관할권을 가지고 있다.
#(X)	X는 이전에 보낸 적이 없는, 최근에 생성된 값이다.
$P \overset{k}{\leftrightarrow} Q$	P와 Q는 키 K를 공유하고 있다.
$\overset{k}{\mapsto} P$	K는 P의 공개키 이다.
$P \overset{X}{\Leftrightarrow} Q$	X는 P와 Q에게만 알려져 있는 비밀 값 이다.
$(X)_K$	X는 키 K로 암호화 된다.
$<X>_Y$	X는 Y와 결합된 값이다.

② 프로토콜의 이상화(Idealized Protocol)

제안한 프로토콜에서 첫 번째 메시지(인증요청||N_{SB1})은 프로토콜의 논리적 속성에 영향을 미치지 않으므로 프로토콜의 이상화 과정에서 생략되었다.

두 번째 메시지 $MSO \rightarrow SB$: $\{N_{MSO1} \| N_{SB1}\}_{K_{MSO}^{-1}}$

세 번째 메시지 $SB \rightarrow MSO$: $\{N_{SB2} \| N_{MSO1}\}_{K_{SB}^{-1}}$

③ 프로토콜의 목표 설정(Protocol Goals)

본 연구에서 제안한 프로토콜이 달성하려는 목표는 MSO와 SB가 상호인증하기 위해서는 각각 생성한 $N_{MSO1}, N_{SB1}, N_{SB2}$ 를 서로 신뢰하고 있어야 한다.

$$MSO \mid\equiv SB \mid\equiv N_{MSO1} \qquad SB \mid\equiv MSO \mid\equiv N_{SB1}$$

④ 프로토콜 검증(Protocol Verification)

두 번째 메시지에서 SB는 공개키 기반 프로토콜에 적용되는 BAN 로직의 추론 규칙 중 '메시지 의미 규칙(Message Meaning Rule)'에 의해 MSO로부터 받은 인증서의 공개키를 이용하여 $(N_{MSO1} \| N_{SB1})$을 볼 수 있다.

$$\frac{SB \mid\equiv \overset{K_{MSO}}{\mapsto} MSO, SB \triangleleft \{N_{MSO1} \| N_{SB1}\}_{K_{MSO}^{-1}}}{SB \mid\equiv MSO \mid\sim (N_{MSO1} \| N_{SB1})} \quad (8)$$

그리고 위 (8)의 결과에 BAN 로직의 추론 규칙 중 "|~" 오퍼레이션과 관련하여 '추가적인 추론 규칙'을 적용하여 SB는 MSO가 N_{SB1}을 보냈음을 알 수 있다.

$$\frac{SB \mid\equiv MSO \mid\sim (N_{MSO1} \| N_{SB1})}{SB \mid\equiv MSO \mid\sim N_{SB1}} \quad (9)$$

위 (9)의 결과와 가정 (6)에 BAN 로직의 추론 규칙 중 '난수 검증 규칙(Nonce Verification Rule)'을 적용하면 다음과 같이 프로토콜의 목표 중 하나인 $SB \mid\equiv MSO \mid\equiv N_{SB1}$을 달성할 수 있다.

$$\frac{SB \mid\equiv \#(N_{SB1}), SB \mid\equiv MSO \mid\sim N_{SB1}}{SB \mid\equiv MSO \mid\equiv N_{SB1}} \quad (10)$$

세 번째 메시지에서 남은 프로토콜의 목표인 $MSO \mid\equiv SB \mid\equiv N_{MSO1}$을 달성하는 과정도 위와 유사하다. 세 번째 메시지에서 MSO는 공개키 기반 프로토콜에 적용되는 '메시지 의미 규칙(Message Meaning Rule)에 의해 SB로부터 받은 인증서의 공개키를 이용하여 $(N_{SB2} \| N_{MSO1})$를 볼 수 있다.

$$\frac{MSO \mid\equiv \overset{K_{SB}}{\mapsto} SB, MSO \triangleleft \{N_{SB2} \parallel N_{MSO1}\}_{K_{SB}^{-1}}}{MSO \mid\equiv SB \mid\sim (N_{SB2} \parallel N_{MSO1})} \quad (11)$$

그리고 위 (11)의 결과에 "$\mid\sim$"오퍼레이션과 관련하여 '추가적인 추론 규칙'을 적용하여 MSO는 SB가 N_{MSO1}을 보냈음을 알 수 있다.

$$\frac{MSO \mid\equiv SB \mid\sim (N_{SB2} \parallel N_{MSO1})}{MSO \mid\equiv SB \mid\sim N_{MSO1}} \quad (12)$$

위 (12)의 결과와 가정(6)에 '난수 검증 규칙(Nonce Verification Rule)'을 적용하면 다음과 같이 프로토콜의 목표 중 하나인 $MSO \mid\equiv SB \mid\equiv N_{MSO1}$을 달성할 수 있다.

$$\frac{MSO \mid\equiv \#(N_{MSO1}), MSO \mid\equiv SB \mid\sim N_{MSO1}}{MSO \mid\equiv SB \mid\equiv N_{MSO1}} \quad (13)$$

이와 같이 본 연구에서 제안한 프로토콜을 BAN 로직으로 정형적 분석 결과, SB와 MSO 간에 안전하게 상호 인증이 수행되었음을 알 수 있다.

5. 결 론

본 논문에서는 XCAS에 적합한 PKI 기반의 장치 인증을 제안하였다. 장치 인증기법을 제안하기 위하여 기존의 공개키 기반 장치 인증기법을 분석하였으며, 이를 기반으로 XCAS에 적합한 PKI기반의 장치 인증을 제안하였다.

인증서 발급 시에 발급 주체, 발급 객체, 제조사 총 3개의 주체가 필요한 것이 일반적이다. 그에 비하여, 제안 하는 셋탑 박스 인증 체계에서는 셋탑 박스에 대한 장치 정보를 담은 셋탑 박스 인증서를 MNF에서 셋탑 박스 제조 시에 직접 저장 하도록 함으로서 방송 서비스용 인증서 발급 시에 MSO와 셋탑 박스 2개의 주체 간에만 통신하도록 구성 되었다. 그로 인해서 데이터 전송 횟수가 현격이 줄어들 뿐만 아니라 MNF와 MSO 간의 통신 망 구축이 필요하지 않기 때문에 효율성이 매우 뛰어나다.

제안한 장치 인증기법을 통하여 XCAS를 구성하는 장치에 대한 안전한 인증을 수행할 수 있을 것으로 기대된다. 이러한 결과물을 통해 XCAS의 보급화 및 활성화에 기여할 수 있을 것으로 기대된다.

참 고 문 헌

[1] OpenCableTM Technical Reports, "DCAS System Overview Technical Report," OC-TR-DCAS-D02-060912, 2006.

[2] NCTA, "Report of the National Cable & Telecommunications Association on Downloadable Security," 2005.

[3] http://www.opencable.com/dcas

[4] http://www.klabs.re.kr

[5] Ki Woong Park, Hyun Jin Choi, and Kyu Ho Park, "Intuitive interface device for wearable computers," in Internation Conference on Next Generation PC, 2005.

[6] Jin-Bum Hwang, Do-Woo Kim, Yun-Kyung Lee and Jong-Wook Han, "Two Layered PKI Model for Device Authentication in Multi-Domain Home Network," Consumer Electronics, 2006. ISCE '06. 2006 IEEE Tenth International Symposium on, 2006.

[7] 주식회사 데이콤, "이동 단말에서 마이크로 익스플로워를 이용한 공개키인증시스템 및 인증 방법", 2000.

[8] 삼성전자 주식회사, "인증서를 이용한 기기 인증 방법 및 상기 방법을 이용하여 기기 인증을 수행하는 디지털 컨텐츠 처리 기기", 2003.

[9] 한국전자통신연구원, "P2P 네트워크에서 보안통신을 위한 키 관리 방법 및 이를 위한 장치", 2006.

[10] 삼성전자주식회사, "이동통신망에서 공개키 기반구조를 이용한 아이피 보안터널의 보안 방법 및 장치", 2005.

[11] 에스케이 텔레콤주식회사, "유무선 통신망에서 무선 통신 단말기의 인증/과금 시스템 및 방법", 2002.

[12] 주식회사 한마로, "인증서를 이용한 디지털 콘텐츠 인증 및 제어 시스템", 2004.

[13] 방송통신위원회, "2008년 방송산업 실태조사 보고서", 2008

[14] 국가정보원, "국가정보보호백서", 2008.

[15] NIST, "Special Publication 800-57 : Recommendation for Key Management - Part 1: General (Revised)," 2007.

[16] 한국인터넷진흥원, "공인인증업무준칙 Ver 1.5", 2009.

[17] 이종수, 조영상, 이정동, 이철용, "선택기반 확산 모형을 이용한 차세대 대형 TV의 수요예측", 정보통신정책연구 제11권 제4호 pp.57-81, 2007.

[18] Yun-Kyung Lee, Deok Gyu Lee, Jong-Wook Han and Tai-Hoon Kim, "Home Network Device Authentication: Device Authentication Framework and Device Certificate Profile," The Computer Journal 2009 52(8):871-877, 2009.

[19] Yu-na Hwang, Hanjae Jeong, Sungkyu Cho, Songyi Kim, Dongho Won and Seungjoo Kim, "A proposal of appropriate evaluation scheme for exchangeable CAS (XCAS)," Information Security Practice and Experience Conference (ISPEC 2010), Seoul, Korea, March 12-13, 2010, pp.217-228.

[20] 성균관대학교 정보통신기술연구소, "키분배 프로토콜 설계에 관한 연구", pp.138, 1999.

[21] Kyungah Shim, "Unknown key-share attack on authenticated multiple-key agreement protocol," Electronics Letters, Vol.39, pp.38-39, 2003.

[22] D. R. L. Brown and A. J. Menezes, "A small subgroup attack on a key agreement protocol of Arazi," Technical report CORR 2001--50, Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, 2001.

[23] Liqun Chen and Chris J. Mitchell, "Parsing ambiguities in authentication and key establishment protocols," 30th

September 2008.
[24] Dang Nguten Duc and Kwangjo Kim, "Securing HB+ against GRS Man-in-the-Middle Attack," SCIS 2007, 2007.
[25] Chien-Lung Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," Computer Standards & Interfaces Vol.26, Issue 3, pp.167-169, May, 2004.
[26] Narn-Yih Lee and Ming-Feng Lee, "Further improvement on the modified authenticated key agreement scheme," Applied Mathematics and Computation Volume 157, Issue 3, pp.729-733, 15 October, 2004.
[27] J. Reid, J.M.G. Nieto, T. Tang, and B. Senadji. Detecting Relay Attacks with Timing-Based Protocols. Proceedings of the 2nd ACM Symposium on Information, Computer, and Communications Security, 204-213, 2007.

황 유 나

e-mail : ynhwang@security.re.kr
2009년 성균관대학교 자연과학부 수학전공 (학사)
2009년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 정보보호, 보안성평가, PKI 인증, 장치인증, 암호이론, XCAS

정 한 재

e-mail : hjjeong@security.re.kr
2006년 성균관대학교 정보통신공학부(학사)
2008년 성균관대학교 전자전기컴퓨터공학과(공학석사)
2008년~현 재 성균관대학교 휴대폰학과 박사과정
관심분야 : 정보보호, 보안성평가, 무선네트워크, 리버스 엔지니어링

원 동 호

e-mail : dhwon@security.re.kr
1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1985년~1986년 일본 동경공업대 객원연구원
1988년~2003년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년 국무총리실 정보화추진위원회 자문위원
2002년~2003년 한국정보보호학회장
2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원
2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, 정보통신대학원장, 성균관대학교 BK21 사업단장
관심분야 : 암호이론, 정보이론, 정보보호

김 승 주

e-mail : skim@security.re.kr
1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년 한국정보보호진흥원(KISA) 팀장
2004년~현 재 성균관대학교 정보통신공학부 교수
2001년~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현 재 교육인적자원부 유해정보차단 자문위원, 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
2007년~현 재 대검찰청 디지털수사 자문위원, KISA VoIP보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원회 위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET