情報保護學會論文誌
第20卷 第3號, 2010. 6

SRP 기반의 DCAS 상호인증 및 키 관리 기법의 제안*

최 현 우,† 여 돈 구, 장 재 훈, 염 흥 열‡
순천향대학교 정보보호학과

Proposal of a Mutual Authentication and Key Management scheme based on SRP protocol*

Hyun-Woo Choi,† Don-Gu Yeo, Jae-Hoon Jang, Heung-Youl Youm‡
Department of Information Security Engineering, Soonchunhayng University

요 약

제한수신시스템(CAS)은 자격을 갖춘 가입자만이 방송 콘텐츠를 시청할 수 있게 하는 IPTV SCP의 핵심 보안기술이다. 과거 CAS는 가입자의 수신기(STB)에 내장된 하드웨어 형태로 존재하거나 또는 분리 가능한 케이블카드 형태로 존재하는 것이 일반적이었다. 하지만 근래에는 기존 CAS의 보안 문제와 확장성 문제 등으로 인해 네트워크를 통해 가입자의 STB에 내려 받을 수 있는 다운로드 가능 제한수신 시스템(DCAS)에 대한 연구가 활발히 이루어지고 있다. 본 논문에서는 다운로드 가능 IPTV SCP의 대표적인 예인 오픈케이블(OpenCable) 기반 DCAS 시스템의 보안요구 사항을 분석하고, 안전한 DCAS 시스템의 핵심이라 할 수 있는 인증서버(AP)와 수신기의 상호인증 및 키 관리 기법을 제안한다. 또한 제안한 기법을 선행연구와 비교 분석하여 그 우수성을 평가한다

ABSTRACT

Conditional Access System (CAS) is a core security mechanism of IPTV SCP (Service and Content Protection) which enables only authenticated user to be able to watch the broadcasting contents. In the past, it was general that CAS was built in Set-Top Box (STB) as hardware or as a detachable cable card. However, numerous researches in Downloadable CAS (DCAS), where users can download CAS code in their STB through their network, have been recently conducted widely due to the lack of security and scalability problem. In this paper, the security requirements of OpenCable based DCAS which is typical example of downloadable IPTV SCP will be derived, the novel authentication and key management scheme will be proposed by using the Authentication Proxy (AP) which is the core DCAS. Also, the benefits of the proposed system will be evaluated by comparison and analysis with preceding research.

Keywords: IPTV SCP, CAS, DCAS, Mutual Authentication

I. 서 론

오늘날 방송시스템은 기존의 디지털케이블망에서 개방된 인터넷망을 이용하는 IPTV 서비스로 진화하였다. IPTV 서비스란 PC 기반으로 인터넷서비스를 제공하는 통신기능과 다채널 TV 방송 서비스를 제공하는 방송기능이 통합된 방송·통신융합서비스를 의미한다.

이와 같은 IPTV 서비스는 자격을 갖춘 가입자만이 유료 콘텐츠 및 다양한 양방향의 서비스를 이용할 수 있는데, 이를 가능케 하는 기술이 바로 CAS(Conditional Access System)이다. CAS는 IPTV SCP(Service and Content Protection)의 대표

접수일(2009년 10월 28일), 수정일(2010년 1월 8일), 게재확정일(2010년 3월 3일)
* 이 논문은 2010년도 순천향대학교 교수 연구년제에 의하여 연구하였음.
† 주저자, zemisolsol@sch.ac.kr
‡ 교신저자, hyyoum@sch.ac.kr

적인 예로써 방송사업자의 네트워크에 가입한 가입자만이 유료 콘텐츠를 이용할 수 있게 하는 IPTV 보안의 핵심 기술이다. 현재의 CAS는 가입자의 STB (Set-Top Box)에 내장되거나 케이블카드 형태로 수신기에서 탈착 가능하게 되어 있는 것이 일반적이다. 하지만 하드웨어 형태의 CAS는 서비스제공자 및 STB간의 호환성 문제, DRM(Digital Right Management)과 같은 CAS와의 연동 가능한 솔루션을 지원하기 위한 확장성 문제, 그리고 CAS가 보안 취약점이 발생했을 때 STB 혹은 케이블카드 전체를 교환해야 한다는 비용문제와 같이 다양한 문제점이 발생할 수 있다. 따라서 근래에는 서비스제공자의 네트워크로부터 STB에 다운로드 가능한 소프트웨어 방식의 CAS 솔루션인 DCAS(Downloadable CAS)에 대한 연구가 활발히 이루어지고 있다.

DCAS는 다운로드 가능한 IPTV SCP의 대표적인 예로써 기존 CAS의 문제점인 호환성과 확장성을 보완하였지만, CAS 이미지를 다운로드 하기 전에 서비스제공자와 STB의 상호인증이 선행되어야 한다는 점과 공개된 망인 인터넷망을 통하면서도 안전하게 CAS 이미지를 전달할 수 있어야 하는 등의 문제점이 잔재한다. 이 문제점들은 두 개체간의 상호인증과 보안통신을 통해 해결될 수 있다.

따라서 본 논문에서는 오픈케이블 기반 DCAS에서 서비스제공자와 STB 사이의 상호인증 및 키 관리 기법을 제안한다. 또한 현재 연구되고 있는 기법과의 비교 분석을 통해 제안된 기법을 평가한다. 본 논문의 2장에서는 CAS와 DCAS의 구조 및 동작 과정과 기존 선행연구에 대해 살펴보고, 3장에서는 오픈케이블 기반 DCAS의 보안 문제점을 분석한다. 4장에서는 본 논문에서 제안한 상호인증 및 키 관리 기법에 대해 설명하고 5장에서는 2장에서 분석한 선행연구와 본 논문에서 제안된 기법을 비교 분석하여 평가 한다. 그리고 마지막으로 6장에서 결론을 맺는다.

II. 관련 연구

본 절에서는 CAS와 DCAS의 구조 및 동작 과정에 대해서 살펴본다.

2.1 CAS (Conditional Access System)

본 절에서는 CAS 시스템의 구조 및 동작 과정에 대해 살펴본다.

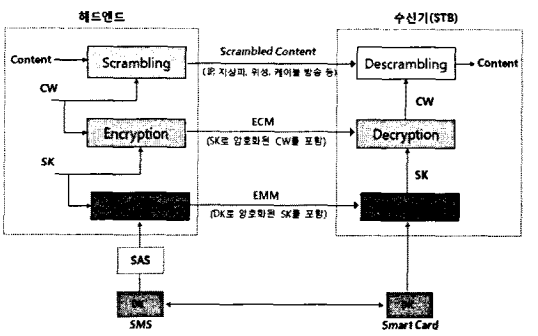
2.1.1 CAS 개요

CAS는 과거 아날로그 방송시스템에서 유료 방송 서비스를 위해 방송 서비스에 대한 고객의 접근 여부를 제어하는 기본 시스템으로 사용되어 왔다[1]. 주로 신호를 스크램블(scrambling) 하여 송출한 뒤 가입자의 STB에서 디스크램블(descrambling) 하는 방식으로 사용된다. 현재 CAS는 가입자의 시청료 납부에서부터 가입자관리시스템(Subscriber Management System, SMS)과 연동을 통해 가입자가 원하는 방송 프로그램을 제공하거나 PPV(Pay Per View), VOD(Video On Demand) 등과 같은 부가서비스를 제공하고 있다.

2.1.2 CAS 구조 및 동작 과정

[그림 1]은 CAS의 구조와 스크램블링/디스크램블링 과정을 보여준다. CAS는 자격관리메시지(Entitlement Management Message, EMM)를 사용하여 수신자격 정보를 전송하고, 자격제어메시지(Entitlement Control Message, ECM)를 사용하여 제어단어(Control Word, CW)와 접근 기준 정보를 전송한다. CW는 실제 콘텐츠의 스크램블링/디스크램블링에 사용되는 대칭키로써 헤드엔드(Head-end)에서 생성된 뒤 서비스키(Service Key, SK)로 암호화되어 ECM을 통해 MPEG-2 전송 스트림과 함께 전송된다. 또한 SK는 가입자 분배키(Distributed Key, DK)로 암호화된 후 EMM을 통해 전송된다. DK는 SMS를 통해 사전에 가입자에게 배포되거나 네트워크로 분배되어 스마트카드 안에 내장되어 있는 키이다.

한편, STB에서 콘텐츠의 디스크램블링은, 수신된 EMM과 ECM으로부터 CW를 복호화함으로써 이루



[그림 1] CAS 구조 및 동작 과정

어질 수 있다. 먼저 STB에 있는 DK를 통해 EMM 메시지의 SK를 복호화하고, 복호화된 SK로 ECM 메시지의 CW를 복호화한다. 그리고 복호화된 CW를 이용하여 암호화된 콘텐츠를 복호화함으로써 디스크램블링 과정을 마치게 된다.

2.2 DCAS (Downloadable CAS)

본 절에서는 오픈케이블(OpenCable) 기반 DCAS 시스템의 구조 및 동작 과정에 대해 살펴본다.

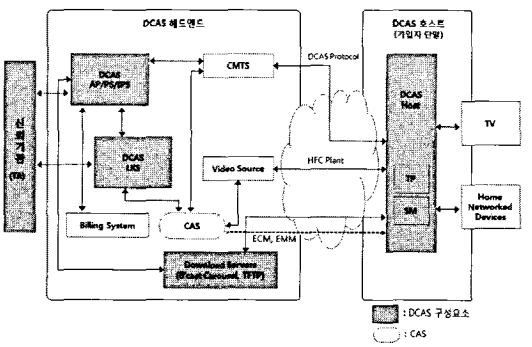
2.2.1 DCAS 개요

오픈케이블 DCAS는 미국 케이블 표준화 기구(CableLabs)의 규격으로써 서비스제공자가 제공하는 CAS가 사전에 STB에 설치되어 있는 것이 아니라, STB가 서비스제공자의 네트워크에 연결 될 시에, 인증절차를 거친 후 CAS 클라이언트 이미지를 STB에 내려 받게 하는 방식이다. 오픈케이블 DCAS는 2004년 8월에 제안되었으며, 2006년 2월에 드래프트 문서가 공개되었고, 현재까지도 DCAS 규격에 대한 표준화가 진행 중에 있다[2].

2.2.2 DCAS 구조 및 동작 과정

DCAS는 [그림 2]와 같이 서비스제공자 네트워크인 헤드엔드(DCAS Head-end)와 가입자의 수신기(DCAS Host), 그리고 신뢰기관(Trust Authority, TA)으로 구성된다.

DCAS 헤드엔드의 PS(Provisioning System)는 SM(Secure Micro) 클라이언트 이미지 다운로드 정책 및 다운로드 스케줄링 정보를 관리하고, IPS (Integrated Personalization Server)는 모든



[그림 2] DCAS 구조

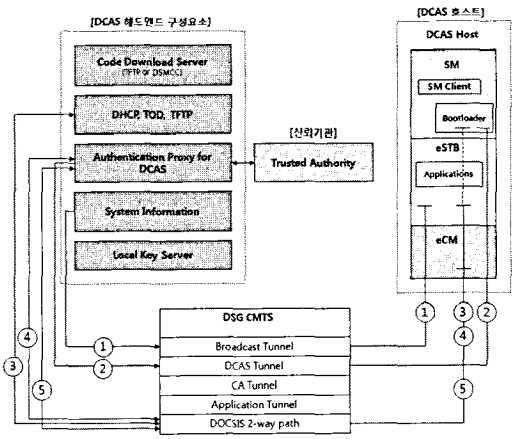
SM 클라이언트 이미지들에 대한 배포, 다운로드, 관리 등을 수행한다. 또한 LKS(Local Key Server)는 DCAS 헤드엔드 내의 키 정보와 비밀 정보 등을 보관·관리하는 기능을 수행한다.

DCAS 호스트는 SM(Secure Micro)과 TP (Transport Processor)라는 전용 칩을 사용한다. SM은 실제 CAS 클라이언트와 같은 SM 클라이언트들이 다운로드 되는 곳이며, 다운로드 된 SM 클라이언트를 부팅시키기 위한 부트로더(Bootloader)와 메시지들을 모니터링하기 위한 DCAS 모니터를 포함한다. 또한 DCAS 헤드엔드의 AP와 인증을 위해 키 관리와 수신된 ECM, EMM 으로부터 복호화키를 추출하여 TP로 전달해 주는 기능을 수행한다. TP는 SM으로부터 전달 받은 복호화키를 이용해 실질적으로 암호화되어 수신된 콘텐츠를 복호화하는 역할을 수행한다. TP는 여러 SM 모듈과의 호환성을 위해 다수의 암호 알고리즘을 포함할 수 있다. 이 외에도 DCAS 헤드엔드와 DCAS 호스트의 각 구성요소들은 다양한 기능을 수행하는데, 자세한 설명은 [표 1]에 나타냈다.

한편, DCAS 호스트가 CAS 모듈과 같은 SM 클라이언트를 요청하면 DCAS 헤드엔드의 AP와 DCAS

[표 3] DCAS 구성요소의 기능 및 특징

DCAS	구성요소	기능 및 특징
DCAS 헤드엔드	AP	·SM 인증, 보안 세션 구성 ·TA와 연동
	LKS	·DCAS 헤드엔드 보안 정보 보관 관리 ·AP의 논리적인 서버로 존재하거나 혹은 별도의 서버로 존재
	PS	·CAS, DRM, ASD 클라이언트들을 저장 ·모든 SM 클라이언트 이미지에 대한 배포, 다운로드, 관리 ·Carousel, TFTP, HTTP 등을 통한 SM 클라이언트 이미지 전달
	IPS	·SM 클라이언트 이미지 다운로드 정책 및 다운로드 스케줄링 정보 생성 및 관리
DCAS 호스트	TP	·SM으로부터 키를 전달 받아 디스크램블링 과정 수행 ·다양한 암호 알고리즘 내장(AES, DES, 3DES, DVB-CAS 등) ·콘텐츠를 재분배하기 위한 암호화 기능
	SM	·보안이 보장되는 칩 ·DCAS 헤드엔드와 상호인증 ·SM 부트로더 내장 ·SM 클라이언트 다운로드 ·SM 클라이언트 저장 및 구동



[그림 3] DCAS 시스템 동작 과정

호스트는 TA와 연동하여 상호인증을 수행 하고, 상호인증이 이루어지고 나서야 SM 클라이언트를 다운로드 할 수 있게 된다. 다음 [그림 3]은 DCAS 호스트가 SM 클라이언트를 다운로드 하는 과정을 보여준다.

① eSTB(embedded STB)는 브로드캐스트 터널(Broadcast Tunnel)을 통해 서비스 정보(Service Information, SI)를 수신한다.

② AP는 DCAS 터널(DCAS Tunnel)을 통해 SM에게 SM 클라이언트의 정보 수집을 위한 명령을 전송한다.

③ eCM(embedded Cable Modem)과 eSTB는 IP 주소를 획득하고, 설정 파일(Configuration File)을 수신한다.

④ SM과 AP는 상호인증을 수행 한다. 또한 이때 ②에서 수신한 정보를 토대로 SM 클라이언트의 정보를 확인한다.

⑤ SM에 설치된 SM 클라이언트가 없거나, 또는 새로운 SM 클라이언트를 설치해야 할 상황이라면, SM은 AP로 SM 클라이언트를 요청하여 새로운 SM 클라이언트를 다운로드 받는다.

위의 ①~⑤단계를 거쳐 SM 클라이언트의 다운로드가 완료되면, SM은 SM 클라이언트의 설치상태 정보를 AP로 전송한다. 그 뒤, DCAS 호스트는 새로운 SM 클라이언트를 위해 리부팅 됨으로써 IPTV 서비스를 위해 동작하게 된다.

2.3 선행 연구

본 절에서는 선행 연구된 DCAS 시스템의 상호인증 및 키 관리 기법에 대해 살펴본다.

2.3.1 디지털케이블 방송망에서 Downloadable 제한수신시스템을 위한 X.509 인증서 기반의 상호인증 및 키 공유 방법[5]

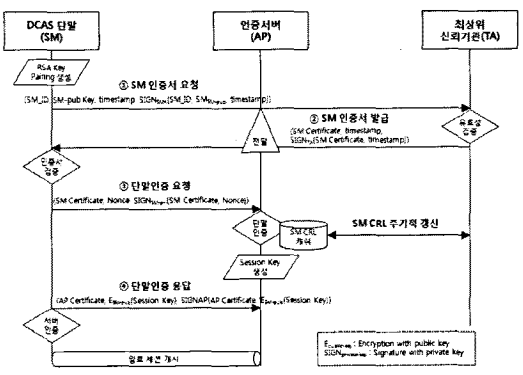
김순철 등은 인증 서버와 단말 간 안전한 보안 통신을 위해 X.509 인증서 기반의 상호인증 방식을 제안했다. 제안한 X.509 인증서 기반의 상호인증 방식은 보안 강도가 높은 인증 방식을 제공하는 반면, 타 방식에 비해 유지 관리 비용 면에서 추가 부담이 요구되는 단점이 있다.

다음 [그림 4]는 X.509 인증서 기반의 DCAS 헤드엔드(AP)와 단말(SM)간의 상호인증 프로토콜을 보여준다.

[그림 4]에서 SM은 제조 시에 TA로부터 발급받은 서명용 인증서와 TA인증서를 가지고 있으며, AP와 TA는 신뢰관계를 구축하고 있다. 자세한 프로토콜 절차는 아래와 같다.

① SM은 RSA(Rivest Shamir Adleman) 알고리즘을 이용해 공개키/개인키 쌍(SM-pub key/SM-pri key)을 생성한 후, TA에게 SM 인증서 요청 메시지를 전송한다. SM 인증서 요청 메시지는 SM의 고유 식별 값(SM_ID)과 SM 공개키(SM-pub key), 타임스탬프(timestamp), 그리고 서명값(SIGNSMK)을 포함한다.

② TA는 SM 인증서 요청 메시지를 수신하고, 자신에 데이터베이스에 있는 SM의 서명용 SM 인증서와 비교하여 SM의 유효성을 검증한다. 검증이 완료된 후, TA는 SM에게 인증용으로 발급한 SM 인증서(SM Certificate)와 타임스탬



[그림 4] X.509 인증서 기반의 DCAS 헤드엔드(AP)와 단말간의 상호인증 흐름[5]

프(timestamp), 그리고 서명값(SIGNTA)을 포함한 SM 인증서 발급 메시지를 전송한다. 이때, SM 인증서에는 인증서버(AP)의 식별정보가 포함된다.

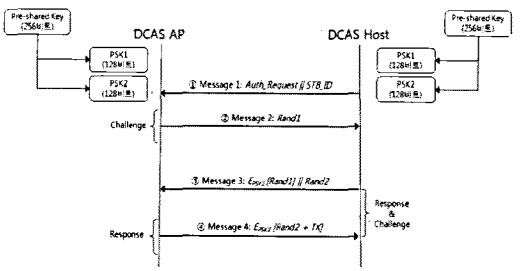
③ SM은 TA로부터 발급받은 SM 인증서를 자신이 가지고 있는 TA 인증서로 검증 한다. 발급 받은 SM 인증서에는 AP의 식별정보가 들어있기 때문에, SM이 상호인증을 수행하고자 하는 인증서버의 실제 정보를 획득하게 된다. 이러한 SM 인증서를 기반으로 SM은 AP에게 단말인증 요청 메시지를 전송한다. 이때 메시지는 SM 인증서와 Nonce값, 그리고 서명값(SIGNSM-pri)을 포함한다.

④ AP는 SM로부터 수신한 SM 인증서의 유효성을 TA 인증서와 인증서취소리스트(Certification Revocation List, CRL) 정보를 이용하여 SM을 인증한다. SM 인증이 완료되면, 보안 통신을 위한 세션키(Session Key)를 생성하고, 생성된 세션키를 SM 인증서의 공개키(SM-pub)로 암호화(ESM-pub(Session Key))한 값과, AP의 인증서(AP Certificate), 그리고 서명값(SIGNAP)을 포함하는 단말인증 응답 메시지를 SM으로 전송한다. SM은 메시지에 포함된 AP 인증서를 참조하여 AP 식별정보와 TA로부터 발급받은 SM 인증서에 포함된 AP 식별정보를 비교하여 AP를 인증하게 된다.

위의 ①~④단계를 거쳐 DCAS 단말과 인증서버는 상호인증을 완료하고, 공유된 세션키를 이용해 암호화 세션을 시작할 수 있다.

2.3.2 안전한 다운로드 가능 제한 수신 시스템 제안 및 구현[7]

강성구 등은 오픈 케이블 기반의 DCAS 시스템의 취약성을 분석 및 보완하여 안전한 DCAS 시스템을 제안하였다. 제안한 논문에서는 DCAS AP와 DCAS 호스트의 상호인증뿐만 아니라, DCAS PS와 DCAS 호스트의 상호인증 기법도 제안하였다.



(그림 5) DCAS AP - DCAS Host 상호인증[7]

아래 (그림 5)는 Challenge-Response 방식을 따르는 DCAS AP와 DCAS 호스트의 상호인증 과정을 나타낸다.

DCAS AP와 DCAS 호스트는 사전에 PSK (Pre-Shared Key)를 공유하고 있다. DCAS AP와 DCAS 호스트의 구체적인 상호인증 과정은 다음과 같다.

① AP와 Host는 PSK를 2개로 분리하여 PSK1과 PSK2를 생성한다. Host는 AP에게 Message 1을 전송한다.

② AP는 Challenge 값 Rand1을 포함하는 Message 2를 Host에게 전송한다.

③ Host는 EPSK1(Rand1)과 같이 Reponse 값을 생성하고, Response 값과 함께 AP 인증을 위해서 Challenge 값 Rand2를 전송한다.

④ AP는 EPSK1(Rand1)을 검증함으로써 Host를 인증한다. 그리고 Host가 전송한 Challenge 값에 대해 EPSK2(Rand2+TK)와 같이 Reponse 값을 생성하여 DCAS 호스트에게 전송한다. Host는 EPSK2(Rand2+TK)를 검증함으로써 AP를 인증하게 된다.

위와 같이 ①~④단계를 거쳐 DCAS AP와 DCAS 호스트는 상호인증을 완료하게 되며, 공유된 임시키인 TK(Temp Key)를 이용해 암호화 세션을 시작할 수 있다.

III. DCAS 시스템의 보안 이슈 분석

본 절에서는 오픈케이블 기반 DCAS 시스템의 보안 이슈에 대해 분석한다.

3.1 오픈케이블 기반 DCAS 시스템의 보안 취약점

오픈케이블(OpenCable) 기반 DCAS 시스템 규격에서는 DCAS 헤드엔드와 DCAS 호스트와의 구체적인 상호인증 메커니즘에 대한 정의가 없다. 그리고 전송 도중에 발생할 수 있는 위변조 방지를 위해 전자서명을 사용하여 SM 클라이언트에 대한 송신자 인증 및 무결성을 제공하도록 규정하고 있지만, SM 클라이

언트를 암호화 하지 않으므로 기밀성은 보장하지 않는다[3]. 이것은 악의적인 공격자가 불법적인 도청으로 SM 클라이언트를 획득 했을 때, 역공학 공격으로 SM 클라이언트를 쉽게 분석할 수 있다는 취약점을 지니게 한다. 게다가 CAS를 위한 분배키와 같이 DCAS 헤드엔드와 DCAS 호스트 사이에 분배되어 공유되어야 하는 키들에 대한 관리 규정이 정의 되어 있지 않다.

아래는 오픈케이블 기반 DCAS 시스템의 보안 취약점을 분석한 표이다.

3.2 오픈케이블 기반 DCAS 시스템의 보안 요구사항

본 절에서는 3.1절의 분석과 [표 2]를 토대로 하여 DCAS 시스템의 보안 요구사항을 도출한다.

3.2.1 DCAS 헤드엔드와 DCAS 호스트간의 상호인증

현재 오픈케이블 기반 DCAS 규격에는 DCAS 시스템의 상호인증에 관여하는 AP와 SM과의 인증 메커니즘이 구체적으로 정의되어 있지 않다. 다만 DCAS 드래프트 문서에서는 상호인증을 위하여 AP와 SM이 사전에 오프라인 등의 방식으로 분배되어 공유된 PSK를 이용하도록 만 규정 하고 있다. 따라서 DCAS 헤드엔드의 AP와 DCAS 호스트의 SM 사이에 상호인증이 가능한 구체적인 메커니즘이 필요하다.

3.2.2 SM 클라이언트의 기밀성 및 무결성 확보

오픈케이블 기반 DCAS 규격에서는 다운로드 되는 SM 클라이언트에 대해 전자서명을 통해서 그 신뢰성을 보장하도록 하고 있다. 하지만 SM 클라이언트는 공개된 인터넷망을 통해 다운로드 되어야 하므로 공격자의 도청과 같은 공격에 대비하기 위해 기밀성을 보장받을 수 있어야 한다. 또한 다운로드 되는 SM 클라이언트의 위변조를 방지하기 위해 무결성 또한 보장되어야 한다. 이는 SM 클라이언트를 암호화하고 암호화된 SM 클라이언트에 대한 해쉬값을 계산하여 첨부함으로써 해결될 수 있다.

[표 2] 오픈케이블 기반 DCAS 시스템의 보안 취약점

보안 취약점	설 명
위장 공격	·불법적인 호스트가 정상적인 DCAS 호스트로 위장할 수 있다. ·불법적인 호스트가 정상적인 AP로 위장할 수 있다.
역공학 공격	·암호화되지 않고 전송되는 SM 클라이언트는 공격자의 역공학 공격에 의해 쉽게 분석될 수 있다.
키 유출	·CAS를 위한 분배키가 고정되어 있어 공격자에 의해 유출될 수 있다.

3.2.3 DCAS 시스템 키 관리

오픈케이블 기반 DCAS 규격에서는 사전에 공유된 PSK를 AP와 SM이 각각 공유하고 있다. DCAS 시스템의 구현을 위해서는 공유된 PSK를 이용하여 향후 암호화와 무결성, 그리고 CAS 시스템을 위한 키들을 생성하고 분배하여야 한다. DCAS 시스템을 위해 필요한 키들은 CAS 클라이언트를 암호화하기위한 키와 무결성 검증을 위한 키, 그리고 CAS 시스템을 위한 분배키 등이다. DCAS 시스템을 위해서는 이들 키들에 대한 효율적인 분배 방법 및 키 관리 메커니즘이 정의되어야 한다.

IV. DCAS 시스템의 상호인증 및 키 관리 기법 제안

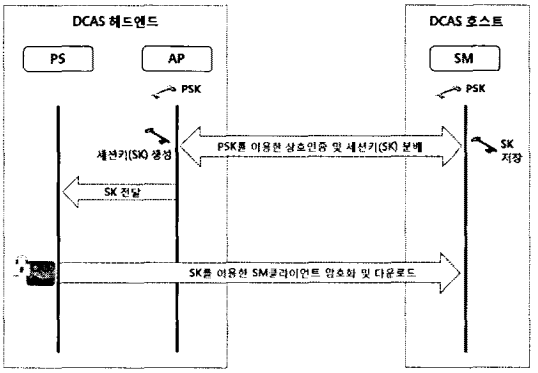
본 절에서는 다양한 방법으로 제안한 DCAS 시스템의 상호인증 및 키 관리 기법의 구현 형태에 대해 분석하고, SRP 프로토콜을 기반으로 하는 안전한 DCAS 시스템을 위한 상호인증 및 키 관리 기법을 제안한다.

4.1 DCAS 시스템의 상호인증 및 키 관리 기법의 구현 형태

본 절에서는 다양한 방법으로 제안한 DCAS 시스템의 상호인증 및 키 관리 기법의 구현 형태에 대해서 분석한다. 본 절에서 제안한 세 가지의 구현 형태는 Pre-Shared Key 기반 방법, 신뢰기관을 이용한 Pre-Shared Key 기반 방법, 그리고 신뢰기관을 이용한 인증서 기반 방법이다.

4.1.1 Pre-Shared Key 기반 방법

Pre-Shared Key 기반 방법은 DCAS 헤드엔드와 DCAS 호스트가 사전에 공유한 키를 이용해 상호인증을 하고 키를 분배하는 방법이다. Pre-Shared Key 기반 방법은 구현이 단순하다는 장점이 있지만, PSK가 고정되어 있어 DCAS 호스트는 DCAS 헤드엔드에 종속 적이며 DCAS 호스트의 서비스제공자가



〔그림 6〕 Pre-Shared Key 기반 방법

변경되는 것과 같은 상황에 대처하기가 미흡하다는 단점이 있다. 다음 〔그림 6〕은 Pre-Shared Key 기반 상호인증 및 키 분배의 형태를 나타낸다.

〔그림 6〕에서 AP와 SM은 사전에 공유된 PSK를 이용하여 상호인증 과정을 거친 뒤, SM 클라이언트를 암호화하기 위한 세션키(SK)를 분배한다. AP는 SK를 PS 서버에 전달하고, PS 서버는 SM 클라이언트를 암호화하여 SM에게 전송한다. 그 후 SM은 암호화된 SM 클라이언트를 PSK를 이용하여 복호화한 후 정상적인 CAS 시스템을 구동할 수 있다. 2.3.2 절에서 소개된 선행연구〔7〕가 Pre-Shared Key 기반 방법에 속한다.

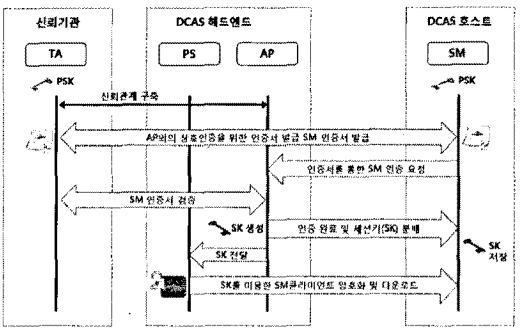
4.1.2 신뢰기관을 이용한 Pre-Shared Key 기반 방법

신뢰기관을 이용한 PSK 기반 방법은 Pre-Shared Key 기반 방법에 신뢰기관이 추가된 형태로써, SM과 AP가 사전에 PSK를 공유하는 것이 아니라, SM과 신뢰기관이 사전에 PSK를 공유하여 상호인증 과정을 수행한다. PSK는 수신기가 제조될 당시에 신뢰기관에 등록되거나, 사용자가 수신기를 구입한 후 오프라인 방식으로 신뢰기관에 등록 시킬 수 있다. 이 방법은 DCAS 헤드엔드 내에 DCAS 호스트들에 대한 PSK를 보관할 필요가 없어, 보안성이 향상된다는 장점이 있다. 하지만, Pre-Shared Key 기반 방법에 비해서 프로토콜의 구현이 복잡해진다는 단점이 존재한다.

4.1.3 신뢰기관을 이용한 인증서 기반 방법

신뢰기관을 이용한 인증서 기반 방법은 인증기관(TA)이 AP와 SM 사이의 상호인증 과정에 개입한다. 인증서 기반의 방법에서는 TA와 SM이 사전에 키를 나눠 갖는 것이 아니라, X.509 인증서 등의 인증서를 나눠 갖고 있다. 이렇게 함으로써 DCAS 헤드엔드 및 DCAS 호스트에 대한 전자서명이 용이하며, DCAS 단말이 서비스제공자를 쉽게 변경할 수 있게 해준다. 또한 DCAS 호스트의 PSK를 DCAS 헤드엔드가 보관할 필요가 없기 때문에 보안성이 향상된다. 하지만, 인증서 기반 방법은 인증기관이 상호인증 및 키 분배 과정에 개입함으로써 프로토콜의 구현이 복잡해지며, 인증서 발급 등의 절차가 필요하기 때문에 통신량 또한 이전 두 구현 방법에 비해 증가한다는 단점이 있다. 2.3.1절의 선행연구〔5〕와 참고문헌〔8〕이 신뢰기관을 이용한 인증서 기반 방법에 속한다.

아래의 〔그림 7〕은 신뢰기관을 이용한 인증서 기반 상호인증 및 키 분배 구성도를 나타낸다.



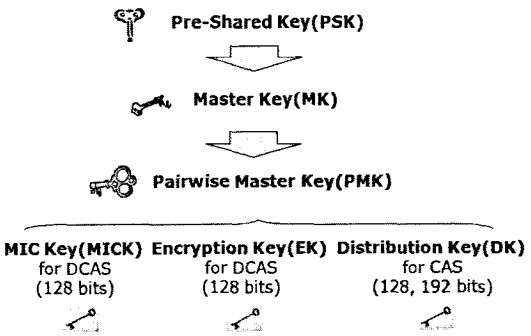
〔그림 7〕 신뢰기관을 이용한 인증서 기반 방법

4.2. SRP 기반 DCAS 시스템의 상호인증 및 키 관리 기법 제안

본 절에서는 SRP 프로토콜에 기반을 두는 안전한 DCAS 시스템을 위한 상호인증 및 키 관리 기법을 제안한다.

4.2.1 제안하는 DCAS 시스템의 키 관리 기법을 위한 계층적인 키 구조

본 논문에서 제안하는 DCAS 시스템의 상호인증 및 키 관리 기법은 〔그림 8〕과 같이 PSK(Pre-Shared Key), MK(Master Key), PMK(Pairwise Master Key), MICK(Message Integrity code Key), EK(Encryption Key), DK(Distribution Key) 등으로 이루어진 계층적인 키 구조를 지니고 있으며, 각 키는 용도에 맞게 사용된다.



[그림 8] 상호인증 및 키 관리를 위한 계층적인 키 구조

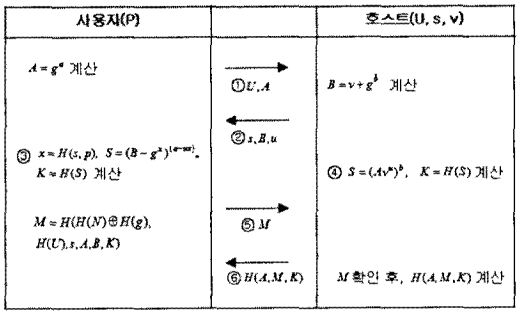
- PSK(Pre-Shared Key)
  DCAS 헤드엔드와 DCAS 호스트가 사전에 공유하는 키이다. 본 논문에서는 DCAS 헤드엔드는 PSK를 가지고 있지 않으며, TA가 각 DCAS 호스트에 해당하는 키 검증자만을 가지고 있다.
- MK(Master Key)
  PSK로부터 PMK를 유도하기 위해 생성되는 임시키이며, AP와 SM의 상호인증 과정에서 생성되는 세션키이다.
- PMK(Pairwise Key)
  MK에 의해서 생성되며, 특정 비트열로부터 EK, MICK, DK를 추출하기 위한 키이다.
- MICK(Message Integrity Code Key)
  다운로드 되는 SM 클라이언트의 무결성을 보장하기 위해 사용되는 키이다. MICK는 PMK로부터 특정 크기의 비트열로 추출된다.
- EK(Encryption Key)
  다운로드 되는 SM 클라이언트의 기밀성을 보장하기 위해 SM 클라이언트를 암호화하는데 사용되는 키이다. EK는 PMK로부터 특정 비트열로 추출된다.
- DK(Distribution Key)
  SM 클라이언트가 DCAS 호스트에 다운로드된 후, 실제 CAS의 동작에서 필요로 하는 키이다. CAS는 DK를 이용하여 콘텐츠의 스크램블링에 사용된 CW를 복호화한다. DK는 PMK로부터 특정 비트열로 추출된다.

4.2.2 DCAS AP와 DCAS 호스트간 상호인증 개요

본 논문에서 제안한 DCAS 시스템을 위한 상호인증은 SRP(Secure Remote Password) 프로토콜에 기반을 둔다. SRP 프로토콜은 상호인증 및 전방향 안전성(forward secrecy)을 제공하는 패스워드 기반 키 교환 프로토콜로써 개체 인증과 함께 세션키 생성이 동시에 이루어진다. SRP 프로토콜은 서버 측에 패스워드 검증자만을 저장하며, 네트워크상으로 패스워드 자체가 전송되지 않아 오프라인 사전 공격에 안전하다. 또한 검증자가 유출되더라도 사전 공격이나 위장 공격과 같은 위협이 존재하지만 키 자체가 유출되는 것이 아니기 때문에 그다지 위협적이지는 않다[4][6].

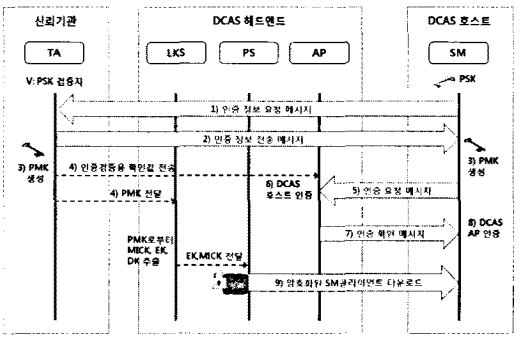
아래는 [그림 9]에 사용된 기호의 설명이며, [그림 9]은 SRP의 동작과정을 나타낸다.

- N : 안전한 큰 소수(N=2q+1, q는 소수)
- g : 모듈로 N상의 원시원소(generator)
- U : 사용자 이름
- p : Cleartext 패스워드
- H() : 일방향 해쉬 함수
- t : 안전성 파라미터
- u : 랜덤 스크램블링 파라미터
- s : 사용자의 salt
- a, b : 비밀값
- A, B : 공개값
- x : 비밀키(p와 s로부터 유추됨)
- v : 패스워드 검증자



[그림 9] SRP 동작 과정

[그림 9]의 동작과정을 간략히 살펴보면, 호스트는 사용자의 패스워드 검증자만을 사전에 저장하고 있으며, 구체적으로 상호인증을 위해 사용자와 호스트가 특정 계산을 위해 필요로 하는 정보들을 주고받는 단계와(①,②), 주고받은 정보를 토대로 미리 정의된 계산과정을 거쳐 세션키를 생성하는 단계(③,④), 그리고 생성된 결과값을 검증하는 단계(⑤,⑥)로 이루어져 있다.



〔그림 10〕 제안하는 상호인증 및 키 분배 개요

〔그림 10〕은 SRP 프로토콜에 기반을 두어 본 논문에서 제안한 상호인증 및 키 분배의 개요를 나타낸다. 본 논문에서는 DCAS 헤드엔드의 서비스시스템들이 신뢰관계에 있으며, 신뢰기관과 AP가 보안채널을 형성하고 있다고 가정한다.

〔그림 10〕의 구체적인 상호인증 및 키 분배 단계는 다음과 같다.

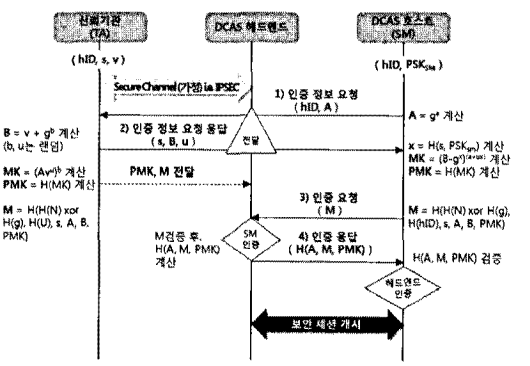
• TA는 DCAS 호스트의 PSK에 해당하는 검증자를 갖고 있다.(사전에 사용자의 DCAS 단말을 TA에 등록하는 과정을 통해 TA에 저장됨)

1) DCAS 호스트는 SM 클라이언트를 다운로드 받기 위해 인증 정보를 요청한다. 이때 DCAS 헤드엔드는 SM 클라이언트의 요청을 TA로 전달한다.
2) 신뢰기관은 DCAS 호스트에 해당하는 인증정보를 전송한다.
3) 신뢰기관과 DCAS 호스트는 인증 정보를 이용하여 계산과정을 거친 뒤 PMK를 생성 한다.
4) 3)의 과정에서 TA는 생성된 PMK를 DCAS 헤드엔드 내의 LKS로, 인증검증용 확인값을 DCAS 헤드엔드 내의 AP로 전달한다.
5) DCAS 호스트는 AP로 인증요청 메시지를 보낸다.
6) DCAS AP는 인증검증용 확인값을 이용하여 DCAS 호스트를 인증한다.
7) 6)의 과정을 통해 DCAS 호스트에 대한 인증이 완료되면 AP는 인증확인 메시지를 DCAS 호스트로 전송한다.
8) DCAS 호스트는 인증 확인 메시지로부터 DCAS 헤드엔드를 인증한다.
9) 상호인증 과정이 끝난 뒤, DCAS LKS는 SM 클라이언트를 암호화하기 위한 EK와 무결성 검사를 위한 MICK를 DCAS PS로 분배하고, DCAS PS는 분배된 키를 이용하여 SM 클라이언트를 암호화 하여 DCAS 호스트로 전송한다.

4.2.3 DCAS 헤드엔드와 DCAS 호스트간 상호인증 프로토콜

DCAS 헤드엔드와 DCAS 호스트간의 상호인증 프로토콜은 SRP 프로토콜에 기반하고 있으며, 사전에 TA가 각 DCAS 호스트에 해당되는 비밀키의 검증자를 보관하고 있다는 가정을 전제한다. 이때 비밀키 검증자는 DCAS 호스트가 제조될 당시 신뢰기관에 저장되거나, DCAS 호스트를 구입한 사용자에 의해서 오프라인과 같은 방식으로 TA에 저장될 수 있다고 가정한다. 또한 DCAS 헤드엔드와 TA는 보안채널을 형성하고 있으며, DCAS 헤드엔드 내의 서브시스템들은 신뢰관계를 형성하고 있다고 가정한다. 아래는 〔그림 11〕의 표기법이며, 구체적인 프로토콜은 〔그림 11〕과 같다.

- N : 안전한 큰 소수(N=2q+1, q는 소수)
- g : 모듈로 N상의 원시원소(generator)
- hID : DCAS 호스트의 식별자
- PSKSM : DCAS 호스트만이 가지는 비밀키
- H() : 일방향 해쉬 함수
- t : 안전성 파라미터
- u : 랜덤 스크램블링 파라미터
- s : 사용자의 salt
- a, b : 비밀값
- A, B : 공개값



〔그림 11〕 DCAS 헤드엔드 - DCAS 호스트의 상호인증 프로토콜

- x : 비밀키(p와 s로부터 유추됨)
- v : 비밀키(PSKSM) 검증자
- TA는 다음과 같이 사전에 DCAS 호스트의 비밀키인 PSK_{SM}의 검증자 v와, 랜덤수 s, 그리고 hID를 데이터베이스에 저장하고 있다.

$$x = H(s, PSK_{SM}) \quad (s\text{는 랜덤수})$$

- DCAS 호스트는 1)의 단계에서 인증 정보 요청을 위해 hID와 $A(=g^a)$를 전송한다. (a는 램덤수)
- TA는 2)의 단계에서, 랜덤수 s,u와 다음과 같이 계산되어진 B값을 DCAS 호스트로 전송한다.

$$B = v + g^b \quad (b\text{는 랜덤수})$$

- DCAS 호스트는 아래와 같이 x, MK, PMK를 계산한다.

$$x = H(s, PSK_{SM})$$
$$MK = (B - g^x)^{(a+ux)}$$
$$PMK = H(MK)$$

- TA는 아래와 같이 MK, PMK를 계산하고, 계산결과 얻어진 PMK를 DCAS AP로 전달한다.

$$MK = (Av^u)^b,\ PMK = H(MK)$$

- 3)의 단계에서, DCAS 호스트는 DCAS AP로 다음의 계산값인 M을 가지고 인증 요청 한다.

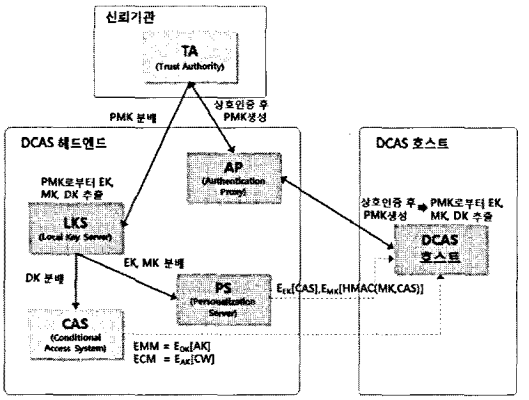
$$M = H(\ H(N) \oplus H(g), H(hID), s, A, B, PMK)$$
(N은큰소수)

- DCAS AP는 수신한 M값을 검증하여 DCAS 호스트를 인증한다.
- DCAS 호스트가 인증이 완료되면, 4)의 단계에서 DCAS AP는 DCAS 호스트로 $H(A,M,PMK)$ 값을 전송하여 응답한다.
- DCAS 호스트는 $H(A,M,PMK)$를 검증하여 DCAS AP를 인증한다.

위의 과정이 끝나면 DCAS 헤드엔드와 DCAS 호스트는 상호인증을 완료하게 되고, EK, MICK, DK를 추출하기 위한 PMK를 공유하게 된다.

4.2.4 DCAS 시스템을 위한 키 분배

본 논문에서 제안한 DCAS 시스템에서는 상호인증 과정 후 생성된 PMK로부터 MICK와 EK, DK를 추출하여 각 용도에 맞게 분배한다. 구체적인 분배 과정은 [그림 12]와 같다.



[그림 12] DCAS 시스템을 위한 키 분배

DCAS 호스트의 SM과 DCAS 헤드엔드의 AP가 상호인증이 완료되면, LKS는 TA로부터 안전한 채널을 통해 PMK를 전달 받고, PMK로부터 EK, MICK, DK를 추출하여 각 용도에 맞게 해당하는 구성요소들로 분배하게 된다.

V. 보안요구 사항 및 성능 평가

보안요구 사항 및 성능 평가 측면에서, 본 논문에서 제안된 기법이 3.2절에서 분석한 DCAS 시스템의 보안 요구 사항을 모두 만족시키고 있음을 [표 3]을 통해 알 수 있다.

본 논문에서 제안한 기법은 DCAS 헤드엔드와 DCAS 호스트간의 상호인증을 제공하며, 전송 중인 SM 클라이언트의 기밀성과 무결성을 제공한다. 또한 인증시 마다 CAS 시스템이 사용하는 DK가 변경되기 때문에, 상호인증 완료 후 타협된 DCAS 호스트가 불법적으로 콘텐츠를 획득하는 것을 방지한다.

성능 평가를 위해, 본 절에서는 2.3절에서 분석한 두 선행연구와 본 논문에서 제안한 SRP 기반 상호인증 및 키 분배 프로토콜을 비교분석 한다. [표 4]은 2.3.1절의 기법(비교기법2)과 2.3.2절의 기법(비교기법1)을 비교분석한 표이다.

먼저, 본 논문에서 다양하게 분류한 구현 형태 측면에서 보면, 비교기법1은 Pre-Shared Key 기반 방법이고, 비교기법2는 신뢰기관을 이용한 인증서 기반 방법이다. 그리고 제안하는 기법은 신뢰기관을 이용한 Pre-Shared Key 기반 방법과 비슷하지만 TA에 PSK대신 PSK의 검증자가 저장된다는 측면에서 신뢰

〔표 3〕 DCAS 시스템의 보안 요구사항 만족

DCAS 보안 요구사항	DCAS 시스템의 보안 요구사항 만족
DCAS 헤드엔드와 DCAS 호스트간의 상호인증	· 제안한 상호인증 프로토콜에 의해서 DCAS 헤드엔드의 AP는 DCAS 호스트의 SM을 인증한다. · 제안한 상호인증 프로토콜에 의해서 DCAS 호스트의 SM은 DCAS 헤드엔드의 AP를 인증한다.
SK 클라이언트의 기밀성 및 무결성 확보	· EK를 통해 다운로드 되는 SM 클라이언트를 암호화함으로써 기밀성이 보장된다. · MICK를 통해 다운로드 되는 SM 클라이언트를 해쉬함으로써 무결성이 보장된다.
DCAS 시스템 키 관리	· 상호인증 과정에서 생성된 PMK는 LKS로 전달되고, LKS는 PMK로부터 EK, MICK, DK를 추출하여 각각의 구성요소들로 분배한다.

〔표 4〕 선행연구와 비교 평가

	비교기법1[7]	비교기법2[5]	제안기법(SRP 기반)
구현 형태	Pre-Shared Key 기반	신뢰기관을 이용한 인증서 기반	신뢰기관을 이용한 키 검증자 기반
인증 주체	헤드엔드-단말	신뢰기관-단말	신뢰기관-단말
키 저장 방식	대칭키	인증서기반 공개키	키 검증자
통신 회수	4회	4회	4회(또는 2회)
세션키 분배	필요	필요	불필요
구현 용이성	매우 용이함	어려움	용이함

기관을 이용한 키 검증자 기반 방법이라 할 수 있다.

본 논문에서 제안된 기법은 신뢰기관을 이용하는 비교기법2와 같이 인증 주체가 신뢰기관과 단말이 된다. 인증 주체가 DCAS 헤드엔드와 단말이 아닌 신뢰기관과 단말이 되는 것은 DCAS 호스트가 DCAS 헤드엔드를 변경할 때나 향후 단말의 로밍 혹은 가입자의 이동과 같이 IPTV 서비스의 이동성을 지원하기 위해서 효과적이다.

다음으로 키 저장 방식 면에서는 대칭키나 인증서 기반의 공개키를 저장하는 방식과 달리 본 논문에서는 단말의 키에 대한 검증자만을 신뢰기관이 저장하고 있다. 키에 대한 검증자만을 저장하는 방식은 네트워크를 통해 키 값에 관련된 정보가 전송되지 않으므로 재전송 공격에 안전할뿐더러, 키 검증자가 유출되거나 손상되더라도 사전 공격이나 호스트 위장 공격과 같은 몇몇 공격이 가능하겠지만 위협을 최소화 할 수 있다는 장점을 가진다.

통신 회수 측면에서는 제안기법이 4회(또는 2회), 비교기법1·2가 각 4회의 통신 회수를 가진다. 제안기법에서는 필요에 의해서 〔그림 11〕의 3)번과 4번 단계를 생략할 수 있다. 3)과 4)의 단계를 생략하게 되면 생성된 세션키를 검증하는 단계만이 사라질 뿐, 여전히 1)과 2)의 단계를 거쳐 생성된 세션키를 통해 암호화 세션은 시작될 수 있다. 따라서 세션키의 검증 절차가 필요 없다면 본 논문에서 제안한 기법은 2회의 통신 회수를 가지게 되어 다른 선행연구들에 비해 효율적이다.

구현의 용이성 측면에서는 인증기관을 필요로 하지 않는 비교기법1이 가장 구현이 용이하며, 신뢰기관을 이용한 인증서 기반 방법인 비교기법2가 가장 구현이 어렵다고 할 수 있다. 비교기법2는 부가적으로 X.509 기반의 인증서 규격을 정의해야 하고, 인증서를 위한 시스템을 구축해야 하므로 구현이 복잡하다. 반면 제안하는 기법은 제3의 신뢰기관만을 필요로 하고 세션키 생성과 계산을 위해 비교적 구현하기 쉬운 멱승, 덧셈, 곱셈, 해킹 등으로 이루어 졌기 때문에, 구현이 용이하다고 할 수 있다.

마지막으로 세션키 분배 측면에서 제안하는 기법은 세션키 분배를 필요로 하지 않는다. SRP 프로토콜의 특성상 상호인증과 동시에 세션키가 생성되기 때문에 세션키를 분배할 필요가 없다.

VI. 결론

CAS 시스템은 기존 하드웨어에 의존한 형태에서 네트워크를 통해 단말에 다운로드 가능한 DCAS 시스템으로 발전하고 있다. DCAS 시스템은 서비스제공자와 단말기 간의 호환성을 제공하고, CAS 클라이언트의 업데이트 및 배포를 용이하게 하며, DRM 등 다른 시스템들과의 연동 또한 쉽게 할 수 있다는 여러

이점을 가진다.

오픈케이블 DCAS 규격은 현재 표준화가 진행 중인 DCAS 시스템의 대표적인 규격이다. 하지만 오픈케이블 DCAS 규격은 DCAS 헤드엔드 및 DCAS 호스트에 대한 보안 요구사항 등과 같이 보안 서비스에 대한 기능을 정의하고 있지 않다. 특히, DCAS 헤드엔드와 DCAS 호스트의 상호인증과 CAS 클라이언트를 보호하기 위한 키 분배 절차에 관한 구체적인 메커니즘이 정의되어 있지 않다.

따라서 본 논문에서는 오픈케이블 기반 DCAS 시스템의 보안 요구사항을 분석하였고, DCAS 시스템을 위한 상호인증 및 키 관리 기법을 제안했다. 본 논문에서 제안한 기법은 SRP 프로토콜에 기반을 두어 안전한 상호인증을 수행 하며, CAS 클라이언트의 암호화 및 무결성에 사용되는 키와 CAS 시스템에서 스크램블링에 사용되는 키를 분배한다. 본 논문에서 제안한 기법은 DCAS 시스템을 비롯하여 IPTV 서비스 보호를 위한 다운로더블 SCP에서 상호인증 및 키 분배에 적용 가능하다. 향후 IPTV 서비스의 활성화에 대비해, 본 논문에서 제안한 기법과 같은 DCAS 시스템을 위한 상호인증 및 키 관리 기법은 안전한 DCAS 시스템을 구현하기 위한 핵심 보안 기능이 될 것으로 기대된다. 또한 앞으로 DCAS 시스템을 비롯한 IPTV 다운로더블 SCP에 대한 연구는 단말의 이동성이라는 특징에 대비하여 서비스제공자 간의 로밍 및 사용자 ID관리 등을 고려하여야 할 것이다.

참 고 문 헌

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

[2] Cable Television Laboratories, Inc., "OpenCable DCAS System Overview Technical Report," OC-TR-DCAS-D01-060 206, Sep. 2006.

[3] OpenCable DCAS Specifications: "Host Device 2.1 Core Functional Requirements," OC-SP-HOST2.1-CFR-I09-090904, Sep. 2009.

[4] T. Wu, "The SRP Authentication and Key Exchange System," RFC 2945, Sep. 2000.

[5] 한국전자통신연구원, "디지털케이블 방송망에서 다운로더블 제한수신시스템을 위한 상호인증 및 키 공유 방법과 장치," 국내특허 공개번호 10-2009-0066178, 2009년 6월.

[6] 김영수, 나중찬, 손승원, "패스워드 인증 프로토콜 동향," 한국전자통신연구원 전자통신동향분석, 16(6), pp. 41-48, 2001년 12월.

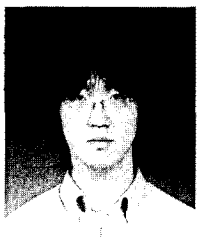
[7] 강성구, 박종열, 백의현, 박춘식, 류재철, "안전한 다운로드 가능 제한 수신 시스템 제안 및 구현," 정보보호학회논문지, 19(6), pp. 161-174, 2009년 12월.

[8] Y.H. Jeong, S.C. Kim, H.J. Kim, H.S. Koo, and U.J. Kwon, "A Novel Protocol for Downloadable CAS," IEEE Transactions on Consumer Electronics, vol. 54, no. 3, pp. 1236-1243, Aug. 2008.

〈著者紹介〉

최 현 우 (Hyun-Woo Choi) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 IPTV 보안, 스마트그리드 보안, USN 보안, 역추적

여 돈 구 (Don-Gu Yeo) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, USN 보안, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적



장 재 훈 (Jae-Hoon Jang) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 역추적, IPTV 보안, USN 보안

염 흥 열 (Heung-Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 졸업(학사)
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장(역), 수석부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
〈관심분야〉 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜