情 報 保 護 學 會 誌
第22卷 第1號, 2012. 2

안전한 콘텐츠 공유를 위한 모바일 IPTV 환경에서 다운로드 가능한 제한수신시스템 (DCAS) 보안 프레임워크 연구

정 영 곤*, 조 효 제* 염 흥 열**

요 약

현재 국내 IPTV 서비스에서는 콘텐츠 보호를 위해 기존 방송 보호시스템인 제한수신시스템(CAS)과 디지털저작권관리(DRM) 기술을 혼용하여 사용하고 있다. 하지만 사용자는 가정의 셋톱박스에서 뿐만 아니라 모바일 단말을 통해서 IPTV 콘텐츠를 시청하고자 한다. 이는 셋톱박스의 콘텐츠나 채널을 모바일 IPTV 와 연계하는 것을 요구한다. 본 논문에서는 모바일 환경에서 셋톱박스에서 공유되는 콘텐츠나 채널을 모바일 단말까지 안전하게 공유하기 위해 요구되는 보안 문제점을 도출하고 이에 따른 보안 요구사항을 도출하며, 이를 기반으로 DCAS(downloadable conditional access system) 을 위한 보안 프레임워크를 제안한다. 또한 기존의 SRP 프로토콜[7]을 기반으로 키 교환 프로토콜을 구성하여 셋톱박스와 모바일 IPTV의 안전한 콘텐츠와 채널의 공유가 가능한 DCAS용 인증 프로토콜을 제안한다.

Ⅰ. 서 론

최근 광대역 네트워크의 발전과 인터넷의 대중화로 인하여 IPTV의 서비스가 전 세계적으로 활성화되고 있다. 네트워크와 멀티미디어 산업의 발달은 통신과 방송의 융합이라는 새로운 형태의 서비스를 탄생시켰다. 대표적인 통신·방송 융합서비스인 IPTV (Internet Protocol TeleVision)는 초고속 인터넷망을 이용하여 가입자의 요청에 따라 방송프로그램을 비롯한 다양한 멀티미디어 콘텐츠를 양방향으로 제공하는 서비스이다[1]. 최근의 IPTV는 QoS(Quality of Service) 가 보장된 광대역 IP 네트워크와 IP 셋톱박스(Set-Top Box), 표준 TV 수상기를 통해서 양방향 TV 서비스를 포함한 디지털 방송 및 통신 융합 서비스를 제공한다. 또한 방송영역에서 제공되던 멀티미디어 콘텐츠를 인터넷 망을 통하여 실시간 전송하는 서비스로 구체화되고 있다[1].

모바일 IPTV는 시간과 장소의 제한 없이 다양한 콘텐츠와 서비스를 제공받을 수 있도록 설계되고 있다. 고정형 IPTV와 달리 모바일 IPTV의 서비스는 디바이스 장치의 물리적인 제약점 (낮은 네트워크 속도, 데이터 처리능력, 한정된 저장공간, 분실 위험성 등)을 극복하기 위한 새로운 요구사항을 충족시킬 수 있는 기술의 개발이 필요하다. 또한 고정형 IPTV의 기능을 모바일 환경에서 안전한 서비스를 제공하기 위한 보안 기술이 개발되어야 한다.

IPTV 서비스의 활성화와 더불어 다양한 서비스 시나리오에서 가입자와 서비스제공자를 보호하고 안전하게 콘텐츠를 제공하기 위한 IPTV 보안 기술의 연구가 활발히 진행되고 있다. IPTV 서비스는 자격을 갖춘 가입자만이 유료 콘텐츠 및 다양한 양방향의 서비스를 이용할 수 있는데, 이를 가능하게 하는 기술이 바로 CAS(Conditional Access System)이다. 방송사업자의 네트워크에 가입한 적법한 가입자만이 유료 프리미엄 등급의 콘텐츠를 이용할 수 있게 하는 CAS는 IPTV

본 연구는 방송통신위원회의 "IPTV 융합서비스 및 콘텐츠 공유를 위한 개방형 IPTV 플랫폼 기술 개발" 원천기술개발사업의연구결과로 수행되었음 (KCA- 2011-09912-03001)
* 순천향대학교 정보보호학과 (ygjung@sch.ac.kr)
** 순천향대학교 정보보호학과 (jyyoum@sch.ac.kr)

SCP(Service and Content Protection)의 요구사항을 만족하는 대표적인 보안 기술이다. CAS와 함께 DRM (Digital Right Management)와 같은 콘텐츠 보안 기술로 콘텐츠에 대한 정당한 사용을 허용해주는 시스템도 존재한다.

이와 같이 IPTV 서비스에서 콘텐츠를 보호하기 위한 기술은 기존 방송시스템에서 사용되던 콘텐츠 보호 기술을 수용하고 이에 더해 새로운 요구사항을 더하여 사용하는 방식이라고 볼 수 있다. 하지만 기존 방송시스템에서 사용되던 보안 기술은 주로 디지털케이블망과 같은 단방향 통신을 위해 설계되었기 때문에 IP 망의 특징인 양방향성을 고려해 볼 때 이를 IPTV 서비스에 대해 적용하는 것은 적합하지 않다 [이유를 설명하면 좋을 듯?]. 또한 모바일 IPTV 서비스의 시작으로 인해 기존의 고정형 IPTV 가입자들을 모바일 IPTV 환경으로 유도하기 위해 새로운 방식의 콘텐츠나 채널의 공유를 위한 추가적인 보안 요구사항을 필요로 한다.

따라서 본 논문에서는 안전한 콘텐츠와 채널의 공유를 위한 모바일 IPTV 보안 모델을 DCAS 방식에 기반을 두고 제시하고, 본 논문에서 제시한 SCP(service and content protection) 프로토콜을 기반으로 한 키교환 프로토콜을 통하여 추가적인 보안 요구사항을 충족한다. 그러한 보안 프레임워크를 운용하기 위해 필요한 보안 요구사항을 도출하고, 이러한 보안 요구사항을 만족시킬 수 있는 모바일 IPTV에서 안전한 콘텐츠 공유를 위한 DCAS 보안 프레임워크를 제안한다.

Ⅱ. 모바일 IPTV

1. 모바일 IPTV 개요

언제 어디서나 모바일을 이용하여 IPTV 서비스를 제공 받을 수 있는 모바일 IPTV 서비스가 제 4세대 이동통신 시스템의 주요 서비스로 등장하게 되었고, 이에 따라 각 기술과 서비스들이 연구 개발되고 있다. 고품질의 영상정보를 모바일로 제공하기 위해서는 무선 액세스망의 성능향상을 위한 다양한 기술들과 IPTV 방송서비스 제어를 위한 IPTV 방송망 구성 및 제어 기술 등이 요구된다. 현재 전세계적으로 이동통신망을 활용한 모바일 IPTV 서비스가 상용화되고 있지 않고 있다. 다음 장에서는 모바일 TV 시스템을 구현하기 위해 이동통신 채널을 이용한 궤환 채널을 부가하여 모바일 IPTV 서비스를 제공하기 위한 기술 개발 현황을 보여준다[3].

2. 모바일 IPTV 기술

2.1 DMB 2.0[17]

국내 6개의 지상파 DMB사들과 이동통신 사업자(SKT, LGT)들은 DMB와 이동통신망의 결합을 통해 모바일 IPTV 서비스를 제공하는 DMB 2.0 서비스를 상용화기술 개발을 추진 완료했다 DMB 2.0에서는 통신망을 활용한 무선인터넷 서비스와 기존의 DMB 서비스를 결합하여 새로운 양방향 서비스를 제공할 예정이다.

DMB 2.0에서는 양방향 서비스를 위해 TV 화면 위에 겹쳐서 데이터서비스를 송출하는 양방향데이터방송(BIFS)과 방송 화면과 별도로 웹브라우저를 구동하는 BWS 등 다양한 방식을 제공할 것이며, 또한, 특정 서비스에 유료로 가입한 단말에게만 서비스를 제공하는 CAS 기술도 적용했다.

2.2 DVB-H[18]

DVB-H는 유럽의 DVB-T 규격을 이동형 방송에 적합하게 성능을 개선한 기술이며, ETSI는 DVB-H를 유럽의 지상파 이동방송서비스 표준으로 채택하였다. 노키아 주도로 시스템을 개발하여 현재 오스트리아, 핀란드, 이탈리아, 스위스, 모로코, 알바니아, 케냐, 나이지리아, 베트남, 필리핀, 인도 등에서 유로로 상용화 서비스를 제공하고 있다. 2011년 DVB-H 성능(SD급 비디오 해상도 지원)을 개선한 DVB-H2(HDTV) 규격 작업을 완료하였으며, 휴대폰, PMP 등 다양한 단말로 DVB-H 서비스를 수신할 수 있다. DVB-H의 주요 특징은 다음과 같다.

- UHF 주파수 대역 사용
- 비디오 코덱: H.264, 오디오 코덱: MPEG-2
- 대규모 광대역 SFN 구성 가능한 규격 채택
- 전송속도: 11Mbps@ 8MHz 대역폭
- Spectral efficiency(bps/Hz): 0.6~2.5
- 13 비디오 채널(video channels) 지원
- IP 기반의 패킷 송신 방식(IP data casting), 궤환

채널로 이동 통신망을 사용하여 양방향 서비스 가능

- 채널 변경 시간: 5초

2.3 ATSC-M/H[19]

미국의 디지털 지상파 방송 규격을 제정하는 미국 TV 표준위원회인 ATSC는 이동성을 지원하는 기능을 대폭 보완하여 미국 모바일 TV의 규격으로ATSC-M/H 표준을 2009년 10월에 완성하였고, 현재 상용화 서비스를 준비 중에 있다. 미국 방송사 사업자들이 주도하는 ATSC-M/H 표준의 수신 단말은 휴대폰, PMP, MP3P, 내비게이션, 노트북, 휴대용 디지털 TV, 자동차용 엔터테인먼트 단말 등 다양하다.

ATSC-M/H 시스템은 기존의 ATSC 시스템과 호환성을 유지하기 위하여 기존의 ATSC 모듈레이터의 일부를 변경하여 이동수신이 가능하도록 재설계하였다. 기존에 할당된 ATSC의 6MHz 대역폭에서 19.39Mbps의 총 전송률을 메인 HDTV 서비스와 모바일-M/H 서비스가 공유하여 사용한다. 따라서 M/H의 서비스가 증가하면 메인 ATSC 서비스에 할당된 대역폭/전송률이 줄어든다. 즉, ATSC-M/H 기술은 메인 서비스를 위한 전송률만 감소시킬 뿐 ATSC 시스템에 어떠한 간섭도 주지 않는다. ATSCM/H는 CIF급 영상 서비스를 지원하고, 광고기반 무료 TV를 기본 서비스로 제공할 계획이며, 또한 정액제 모바일 TV, 주문형 비디오(VOD), 유료 시청(PPV) 서비스, 양방향 TV 및 비실시간 콘텐츠 다운로드 등 다양한 데이터 서비스를 주요 서비스로 고려하고 있다.

ATSC-M/H 기술은 최대 120 KM/h의 이동 속도를 지원하며, 기존의 DTV 주파수를 활용하기 때문에 별도의 주파수 배정이 필요 없다. ATSC-M/H의 주요 기술적인 특징은 다음과 같다.

- 고속 이동 환경 하에서 계속 변하는 채널을 추정하기 위한 훈련신호 제공
- 수신 성능 증대와 전송 중 발생하는 오류에 강하도록 RS(Reed Solomon) 코드와 SCCC () 를 구성하여 채널 부호화 수행
- 16개 사용 가능한 slot들 중 한 개 서비스에 할당 가능한 slot은 최대 8개까지만 가능하며 나머지 slot 동안에는 슬립모드로 전환하는 타임 슬라이싱 기술 적용
- GPS에 의한 동기화 및 모든 패킷에 time stamp를 적용하여 SFN 지원
- 비디오 압축은 H.264/AVC를 지원, 오디오 압축은 HE-AAC/v2 지원

Ⅲ. 보안 문제점 및 보안 요구사항 분석

1. 모바일 IPTV 콘텐츠 공유를 위한 보안 문제점

오픈케이블(OpenCable) 기반 DCAS 시스템 규격에서는 DCAS 헤드엔드와 DCAS 호스트와의 구체적인 상호인증 메커니즘에 대한 정의가 없다[8?]. 그리고 전송 도중에 발생할 수 있는 CAS 클라이언트의 위변조 방지를 위해 전자서명을 사용하여 송신자 인증 및 데이터 무결성을 제공하도록 규정하고 있지만, 클라이언트를 암호화 하지 않으므로 기밀성은 보장하지 않는다[8]. 오픈케이블에서 규정되지 않은 키관리, 인증 등과 같은 사항들을 구체화할 필요가 있다. 악의적인 공격자가 호스트로 위장하여 콘텐츠를 불법적으로 취득하거나 다운로드하여 비인가된 방법으로 클라이언를 취득하여 이에 대해 역공학 공격을 수행해 클라이언트의 분석이 가능할 수 있다. 또한 키교환을 정의하지 않아 안전하지 않은 키교환 프로토콜 사용시 키 유출의 위험이 따르게 된다. 이러한 위협을 바탕으로 안전한 콘텐츠의 공유를 위한 모바일 IPTV 환경에서 발생 가능한 문제점을 분석한다.

1.1 키 관리

DCAS의 안전한 사용을 위해 DCAS 서버와 모바일상의 DCAS 호스트 간의 상호인증을 위해서 PSK (Pre-Shared Key)는 반드시 안전한 방법으로 각 개체로부터 분리된 별도의 하드웨어 토큰을 이용해야 한다. 하지만 오픈케이블에서는 이러한 키 분배를 정의하고 있지 않다. 또한 휴대가 용이한 모바일의 특성으로 인해 셋톱박스와는 달리 스마트카드와 같은 키 저장 매체를 사용하는데 어려움이 있고 단말 분실의 위험성까지 존재하여 모바일 단말에 키의 저장은 많은 위험을 내포하게 된다.

1.2 위장공격

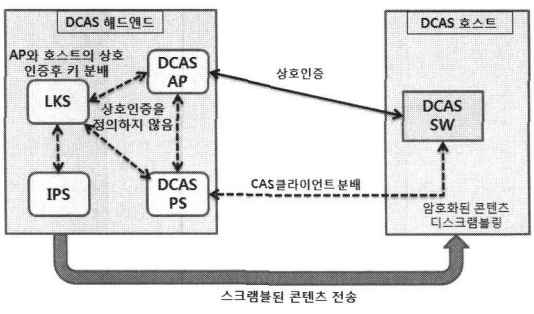
현재 오픈 케이블의 DCAS 규격에서는 DCAS 서버

와 DCAS 호스트가 공유키를 이용해 상호인증을 수행하도록 정의하고 있지만, 구체적인 인증 메커니즘에 대해서는 별도로 정의하고 있지 않다. 특히 DCAS 클라이언트의 다운로드는 DCAS PS에서 다운로드 하게 되어 있는데 DCAS PS와 호스트 간에 인증 방법에 대해서도 정의 되어 있지 않다. 그리하여 악의적인 공격자가 DCAS PS로 위장하여 호스트를 속인후 호스트에게 자신이 프로그래밍한 비정상 DCAS 클라이언트를 다운로드하게 하여 설치하게 한후 악성코드에 감염시킬 수 있는 위협도 존재한다. 다시 말해, 공격자가 DCAS AP로 위장하여 호스트가 적법한 DCAS 클라이언트를 다운로드하는 것을 막고 자신이 작성한 악성코드를 포함한 변조된 DCAS 클라이언트를 다운로드 하게 할 수 있다.

특히, 이러한 공격은 DCAS 해드엔드의 AP와 호스트간의 인증이 완료된 이후에 이루어지기 때문에 위험성이 더욱 크다. 현재 오픈케이블 DCAS 규격에서는 DCAS 시스템의 상호인증에 관여하는 AP와 호스트간의 인증 메커니즘 또한 구체적으로 정의되어 있지 않다. 다만 DCAS 드래프트 문서에서는 상호인증을 위하여 AP와 호스트가 사전에 오프라인 등의 방식으로 분배되어 공유된 PSK만 이용하도록 규정하고 있다.

1.3 DCAS 클라이언트의 보호

오픈케이블의 DCAS 규격에서는 DCAS 서버로부터 다운로드하는 DCAS 클라이언트의 보호 방안에 대해서는 별도로 기술하고 있지 않다. 오픈케이블의 'Common Download' 규격[8]에서는 다운로드 되는 소프트웨어에 단말 제조업체가 전자서명을 첨부하도록 하여 다운로드 되도록 함으로써 소프트웨어의 신뢰성을 보장하도록 하고 있다. 그러나 'Common Download' 규격에서는 전자서명을 통한 소프트웨어의 신뢰성 이외에 콘텐츠의 기밀성을 보장하지는 않는다. DCAS 클라이언트는 공개된 인터넷망을 통해 다운로드 되어야 하므로 공격자의 도청과 같은 공격에 대비하여야 한다.



(그림 1) DCAS 구성요소간 인증

1.4 DCAS 해드앤드 서버 구성요소 간 보호

오픈케이블 규격에서는 DCAS 서버를 구성하고 있는 하위 서버들(DCAS LKS, DCAS AP, IPS, CDAS PS) 간의 보안 서비스에 대해서는 별도로 정의하고 있지 않아 아래와 같은 문제점이 발생한다.

가. 비밀 정보 유출

LKS에는 DCAS AP가 사용하는 모든 키가 저장되어 있다. 또한 다른 서버들 간의 키 교환이 필요하지만 보안 메커니즘이 정의되어 있지 않아 노출의 위험이 있다.

나. 다운로드 정책 유출

다운로드 프로파일, 다운로드 일정 등 다운로드 정책 정보는 IPS로부터 DCAS AP로 전송된다. 이러한 다운로드 정책이 노출되어 유출되었을 경우 공격자는 다운로드 되는 클라이언트를 더욱 쉽게 공격하게 해줄 수 있다.

다. 위장 공격

악의적인 공격자가 DCAS 헤드엔드 서버들 간에 통신 내용을 도청하여 획득한 정보를 이용하여 DCAS AP, DCAS LKS, IPS, DCAS PS 등으로 위장할 수 있다. LKS로 위장하여 DCAS AP와 호스트간의 상호인증을 방해하거나 DCAS AP로 위장함으로써 다운로드 정책을 유출 할 수도 있다.

〔표 1〕 DCAS 구성요소의 기능 및 특징

구성요소	기능 및 특징
AP(Authentication Proxy)	SM 인증, 보안 세션 구성 TA와 연동
LKS(Local Key Server)	DCAS 헤드엔드 보안 정보 보관 관리 AP의 논리적인 서버로 존재하거나 혹은 별도의 서버로 존재
PS(Provisioning System)	CAS, DRM, ASD 클라이언트들을 저장 모든 SM 클라이언트 이미지에 대한 배포, 다운로드, 관리
IPS(Integrated Personlization Server)	SM 클라이언트 이미지 다운로드 정책 및 다운로드 스케줄링 정보 생성 및 관리

2. 보안 요구사항

2.1 기본 보안 요구사항

본 절에서 제시된 보안 요구사항은 "OpenCable DCAS Specification, Host Device 2.5 Core Functional Requirements" [6] 에 기반을 두고 있으며, 기본 보안 요구사항은 다음과 같다.

- 보안 요구사항 1: 호스트는 DOCSIS, OpenCable, OCAP 규격에 따라 플랫폼 코드를 다운로드 할 때, 무결성과 전자서명을 이용한 메시지 인증을 검증해야 한다.
- 보안 요구사항 2: 유효하지 않은 플랫폼 코드로 판단될 경우에는 정해진 규칙에 따라 에러 처리 해야 한다.
- 보안 요구사항 3: 호스트는 전자서명이 첨부되어 있고, 첨부된 전자서명의 유효성이 검증된 플랫폼 코드만을 실행시켜야 한다.
- 보안 요구사항 4: 호스트 플랫폼 코드는 DOCSIS, OpenCable, OCAP에 정의된 바에 따라 RSA 전자서명을 첨부하고 있어야 한다.
- 보안 요구사항 5: 호스트는 코드의 실행 중 변경을 허용하지 않는다.
- 보안 요구사항 6: DCAS AP와 DCAS 호스트는 상호인증을 수행해야 한다.
- 보안 요구사항 7: DCAS PS와 DCAS 호스트는 상호인증을 수행해야 한다.
- 보안 요구사항 8: DCAS AP와 DCAS LKS는 상호인증을 수행해야 한다.
- 보안 요구사항 9: DCAS AP와 DPS는 상호인증을 수행해야 한다.
- 보안 요구사항 10: DCAS AP와 DCAS PS는 상호인증을 수행해야 한다.
- 보안 요구사항 11: DCAS LKS에게 DCAS AP와 TA 와의 통신 이외에 다른 통신은 허용되지 않는다.
- 보안 요구사항 12: DPS는 DCAS AP와의 통신만 허용된다.
- 보안 요구사항 13: DCAS PS는 DCAS AP와의 통신만 허용된다.
- 보안 요구사항 14: DCAS AP와 DCAS LKS간의 통신 내용은 기밀성과 데이터 무결성을 보장해야 한다.
- 보안 요구사항 15: DCAS AP와 DPS와의 통신 내용은 기밀성과 무결성이 보장되어야 한다.
- 보안 요구사항 16: DCAS AP와 DCAS PS 간의 통신 내용은 기밀성과 무결성이 보장되어야 하며, 부인봉쇄가 가능해야 한다.
- 보안 요구사항 17: DCAS PS와 DCAS 호스트 간의 통신내용은 기밀성과 무결성이 보장되어야 하며, 부인 봉쇄가 가능해야 한다.

위의 보안 요구사항들 중, 보안 요구사항 1~5까지는 "OpenCable DCAS Specification, Host Device 2.5 Core Functional Requirements"에서 제시된 보안 요구사항들을 이용했으며, 이 외에 보안 요구사항 6~17까지는 DCAS의 네트워크 보안을 위하여 추가적으로 제시한 보안 요구사항들이다[6].

2.2 추가 보안 요구사항

일반적인 DCAS 시스템에서는 DCAS 호스트가 DCAS 클라이언트를 다운로드하기 위하여 DCAS AP와 DCAS 호스트 간의 상호인증에 사용되는 PSK를 미리 공유하여야 한다. 그리고 콘텐츠 서비스 제공자가 스크램블링하여 전송하는 콘텐츠를 호스트가 디스크램블링하기 위해 필요한 분배키(Distribution Key)를 스마트 카드와 같은 저장 매체를 사용하여 미리 공유/분배해야 한다. 하지만 모바일 기기에서는 스마트 카드와 같은 매체를 읽을 수 없는 제한된 환경이고 분실의 위험이 있어서 이를 모바일 기기 내부의 메모리에 저장하여 사용하기는 위험이 따른다.

사용자만이 소유하고 있는 콘텐츠의 저장은 서비스 제공자의 저장소를 이용하지 않고 자신 만의 저장공간에서 소유할 수 있다. 사용자가 소유한 콘텐츠 전송을 사용자의 셋톱박스에서 직접 전달하여 콘텐츠 서비스 제공자의 저장장치에 저장할 필요가 없다. 그로 인하여 발생하는 셋톱박스와 모바일 기기 사이에서의 안전한 키관리와 콘텐츠의 교환이 요구된다.

위와 같은 보안 요구사항들이 아래의 항목으로 추가적으로 요구된다.

- 보안 요구사항 18: DCAS AP와 DCAS 호스트 간 PSK는 안전하게 공유되어야 한다.

- 보안 요구사항 19: PSK와 DK 정보는 모바일 기기에 저장되어서는 안된다.
- 보안 요구사항 20: 셋톱박스와 DCAS 해드앤드 간 DK는 안전하게 공유되어야 한다.
- 보안 요구사항 21: DCAS 해드앤드와 DCAS 호스트 간 DK는 안전하게 공유되어야 한다.
- 보안 요구사항 22: 셋톱박스와 DCAS 호스트 간 콘텐츠는 안전하게 공유되어야 한다.

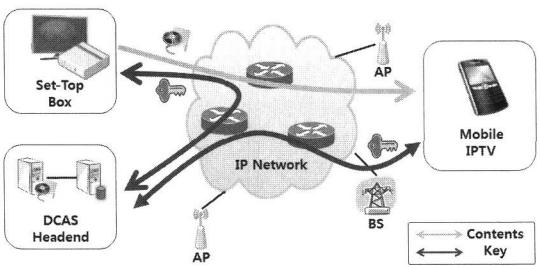
Ⅳ. 보안 프레임워크와 인증 프로토콜 제안

본 장에서는 제 3장에서 분석한 문제점을 바탕으로 보안 요구사항을 만족하는 안전한 콘텐츠의 공유를 위한 모바일 IPTV 보안 프레임워크와 키 교환 프로토콜을 제안한다.

1. 기본구조

본 논문에서 제안하는 안전한 콘텐츠 공유를 위한 DCAS 보안 프레임워크는 사용자만이 소유하고 있는 콘텐츠를 다른 모바일 단말과 함께 공유하는데 요구되는 보안 요구조건을 만족시키는 것을 다룬다. 사용자는 자신이 소유하고 있는 콘텐츠를 다른 모바일 기기에 전송하여 시청을 가능하게 해준다. IPTV 서비스 제공자의 저장소를 이용하지 않고 자신의 셋톱박스에서 자신만의 저장장치에 보관하고 있는 콘텐츠를 공유하는데 목적을 둔다. 위의 <그림 1>은 본 논문에서 제안하는 안전한 콘텐츠 공유를 위한 모바일 IPTV 환경의 DCAS 시스템 키 관리와 콘텐츠의 흐름을 보여준다.

셋톱박스에서 제공되는 사용자의 콘텐츠는 사전에 특정 저장소를 사용할 수도 있고 클라우드 환경에 의해 저장될 수 있다. 오로지 자신만이 가지고 있는 콘텐츠를



〔그림 2〕 모바일 IPTV 콘텐츠 공유와 키 관리

모바일 IPTV 환경에 공유하기 위한 키관리가 필요하다. 사용자가 모바일을 사용하기 위해 접속시마다 매번 새로운 키가 생성되어 안전한 키의 관리가 가능하다.

2. DCAS 보안 프레임워크

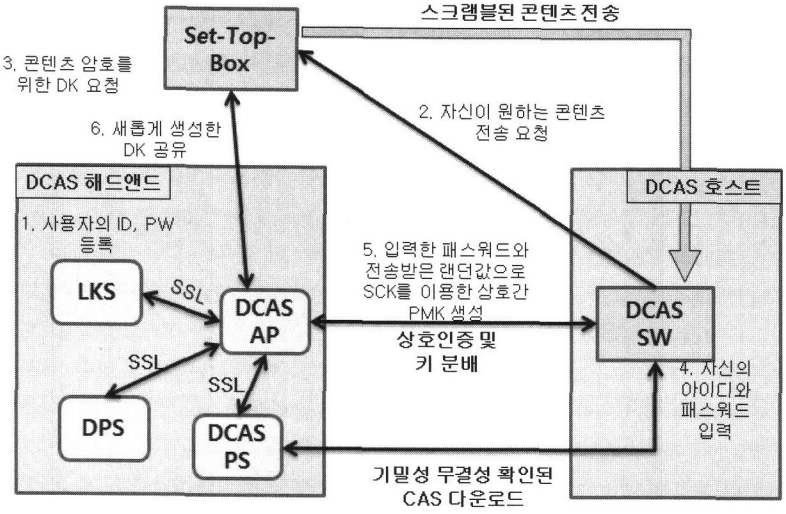
본 절에서는 제 3장에서 분석한 DCAS와 모바일 IPTV의 보안 문제점을 분석하고 보안 요구사항을 만족하는 안전한 콘텐츠의 공유를 위한 DCAS 모바일 IPTV 보안 프레임워크를 제안한다.

<그림 4>은 DCAS 보안 프레임워크로 안전한 콘텐츠 공유를 위한 절차와 구조를 보여주고 있다. 절차는 다음과 같다.

① 사용자는 자신의 ID와 PW를 DCAS 해드앤드에 등록한다.
② 사용자는 자신이 소유한 콘텐츠를 셋톱박스에 요청한다.
③ 셋톱박스는 콘텐츠의 스크램블링에 필요한 일회용 DK를 DCAS 해드앤드에 요청한다.
④ 사용자는 DCAS 해드앤드에 등록한 ID와 PW를 입력한다.
⑤ 입력한 패스워드와 전송받은 랜덤값으로 SRP 프로토콜을 사용하여 공통된 일회용 PMK를 생성한다.
⑥ 공통으로 생성된 일회용 PMK로 생성된 DK (Distribution Key)를 셋톱박스와 공유한다.

본 논문에서 제안한 DCAS 보안 프레임워크를 만족하기 위해 다음과 같은 가정사항을 만족하여야 한다.

- 셋톱박스와 DCAS 해드앤드는 서로 스마트카드와 같은 물리매체로 안전하게 키를 공유하고 있다.
- 셋톱박스는 안전하게 자신의 저장소를 사용하여 콘텐츠를 저장하고 있다.
- 콘텐츠는 비디오 스케일러블 코드에 의해 저장되고 변환 될 수 있다.
- 다양한 패스워드 기반 키 교환 프로토콜이 있지만 본 프레임워크에서는 DCAS 시스템을 위한 상호 인증과 키 생성으로 SRP(Secure Remote Password) 프로토콜을 사용한다[10].
- 또한 키 교환 프로토콜서 결과로 상호간 생성하고 사용되는 PMS는 ITU-T 표준인 X.1193에서 정의한 계층적 키 구조를 사용한다[9]. SCP 프로토콜



〈그림 3〉 모바일 IPTV 환경의 DCAS 보안 프레임워크

과 계층적 키 구조에 대한 자세한 내용은 다음 절에서 다룬다.

본 논문에서 제안한 프레임워크의 동작과정의 자세한 절차는 다음과 같다.

① 사용자는 해드앤드 DCAS의 LSK에 자신이 콘텐츠 공유에 사용할 ID와 패스워드를 등록한다.

② DCAS AP 혹은 DCAS 호스트에 의해서 새로운 DCAS 클라이언트 프로그램의 다운로드를 요청한다.

③ DCAS AP와 DCAS 호스트는 ID와 패스워드를 이용하여 SCP 프로토콜로 생성한 공통의 PMK를 생성한다.

④ DCAS AP와 DCAS 호스트는 공통의 PMK를 통하여 상호인증을 수행하고 PMK로부터 EK, MICK, DK를 추출한다.

⑤ 상호인증이 완료된 후에 DCAS AP는 DCAS PS에게 다운로드 받아야 할 DCAS 호스트의 정보를 전달한다.

⑥ DCAS AP로부터 다운로드를 통보 받은 DCAS PS는 DCAS 호스트와 상호인증을 수행하고, 상호인증이 완료되면 다운로드 될 DCAS 클라이언트를 암호화하는데 사용될 키를 공유하기 위한 EK 키분배 절차를 거친다.

⑦ DCAS PS는 DCAS 클라이언트를 MICK를 이용하여 해쉬하고 EK를 이용하여 암호화하여 DCAS 호스트에게 다운로드 한다. 다운로드가 완료되면 DCAS PS는 DCAS AP에게 다운로드가 완료되었음을 알린다.

⑧ DCAS PS로부터 다운로드가 완료되었음을 통보받은 DCAS AP는 분배키를 셋톱박스에 전달하여 방송 콘텐트를 암호화하는데 사용하도록 한다.

⑨ DCAS AP는 DK의 전달을 위해 미리 공유하고 있는 PSK를 사용하여 안전하게 셋톱박스에 전달한다.

⑩ 셋톱박스는 DK를 이용해서 콘텐츠를 DCAS 호스트에게 전달한다.

3. 인증 프로토콜

3.1 SCK(Secure Common Key) 프로토콜

본 논문에서 제안한 DCAS 보안 프레임워크에 상호인증은 SRP(Secure Remote Password)[?] 프로토콜을 변형한 방식(이후 SCK(Secure Common Key) 프로토콜로 명칭함) 관련 키를 생성한다. SRP 프로토콜은 사용자와 호스트간에 상호인증과 전방향 안전성(forward secrecy)을 제공하는 키 교환 프로토콜이다. SRP 프로토콜의 상호인증과 전방향 안전성으로 개체 인증과 세션키 생성이 동시에 이루어지는 장점이 있다. SRP 프로

〈표 2〉 SCP 프로토콜 기호 설명

기호	설 명
N	안전한 큰 소수(N+2q+1, q는 소수)
g	모듈로 N상의 원시원소(generator)
ID	사용자가 등록한 ID
p	사용자가 등록한 패스워드
H()	일방향 해쉬 함수
t	안전성 파라이터
u	랜덤 스크램블링 파라미터
s	사용자의 salt
a, b	비밀값
A, B	공개값
x	비밀키(p와 s로부터 유추됨)
v	패스워드 검증자

토콜의 가장 큰 특징으로 서버 측에 사용자의 패스워드 검증자만을 저장하여 네트워크상으로 패스워드 자체가 전송되지 않는다. 그러므로 오프라인 사전 공격에 안전하고 검증자가 유출되더라도 사전 공격이나 위장 공격과 같은 위협이 존재하지만 키 자체가 유출되는 것이 아니기 때문에 크게 위협은 되지 않는다[10][11].

본 논문에서 적용한 SCK 프로토콜에서 사용자는 DCAS 호스트가 되고 호스트는 DCAS 해드앤드가 된다. 또한 프로토콜의 기호로 사용되는 U는 사용자의 ID로 되고 p는 패스워드로 사용되어 진다.

위의 <표 2>는 SCP 프로토콜의 동작에서 사용되는 기호들을 설명하고 있다. 그 과정은 다음과 같다.

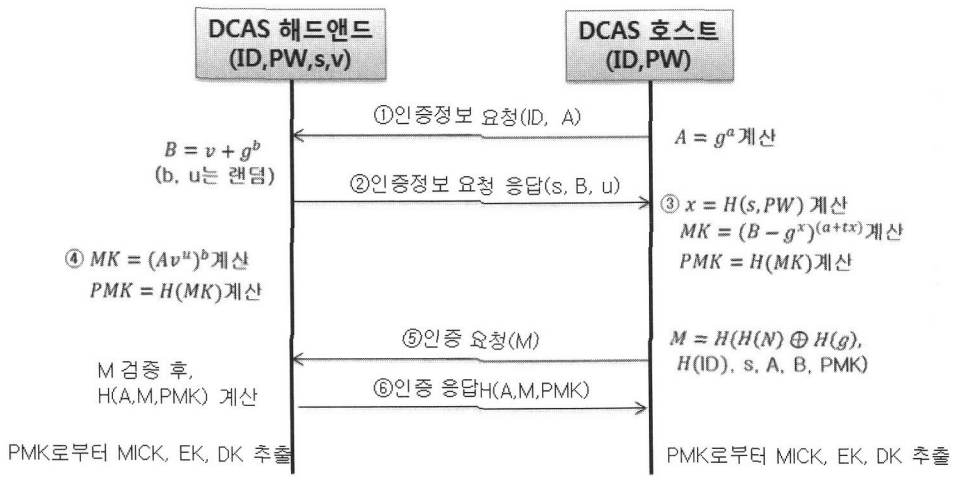
- 호스트는 다음과 같이 패스워드를 저장한다.

$$x = H(s,p) \quad (\text{s는 랜덤하게 선택됨})$$

$$v = g^x$$

- 호스트는 패스워드 데이터베이스에 U, s, v를 저장한다
- 사용자는 호스트에게 신분 증명을 위해 이름과 $A(=g^a)$를 전송한다(여기서 a는 랜덤수)(①)
- 호스트는 salt s와 $B(=v+g^b)$, 그리고 랜덤한 스크램블링 파라미터 u를 사용자에게 전송한다(여기서 b는 랜덤수)(②)
- 사용자는 $x(=H(s,p))$ 와 $S(=(B-g^x)^{(a+ux)})$, 그리고 $K(=H(S))$를 계산한다(③)
- 호스트는 세션키 $S(=(Av^u)^b)$와 $K(=H(S))$를 계산한다. 이로써 양측은 분배된 세션키 K를 갖게 된다. 양측은 인증을 위해 각기 자신들의 키가 매칭됨을 증명할 필요가 있다(④)
- 사용자는 $M(=(H(H(N)\oplus H(g), H(U), s, A, B, K))$을 계산하여 호스트에게 전송한다(⑤)
- 호스트는 받은 M과 세션키를 이용하여 $H(A, M, K)$를 계산하여 사용자에게 전송한다(⑥)

위의 <그림 5>은 SCK 프로토콜의 동작과정은 나타낸 그림이다. 간략하게 ①과 ②의 단계는 상호인증을 위해 사용자와 호스트가 사전 준비로 필요로 하는 정보를 주고받는 단계이다. ③과 ④의 단계는 주고받은 정보를 이용하여 세션키를 생성하는 단계이다. ⑤와 ⑥의

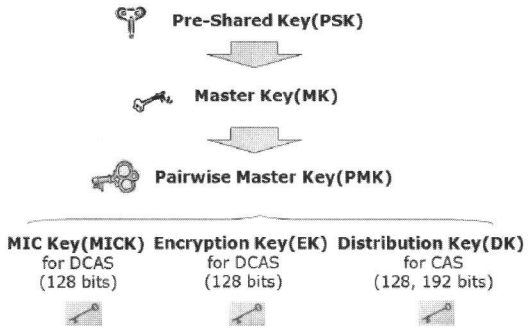


〈그림 4〉 SCK 프로토콜 동작 과정

단계는 사용자와 호스트에서 생성된 결과값을 검증하는 단계이다.

3.2 계층적 키 구조

본 논문에서 제안한 프레임워크에서 사용한 키는 계층적 키 구조를 가지고 있어 DCAS 클라이언트의 기밀성과 무결성을 위한 추가적인 키의 사용이 가능하다는 장점이 있다. 제 3장에서 분석한 DCAS 클라이언트의 기밀성과 무결성을 위한 키로 사용 된다.



〈그림 5〉 계층적 키 구조(X.1193)

위의 <그림 6>은 X.1193에 정의된 다운로더블 SCP를 위한 계층적 키 구조를 보여주고 있다. 이 계층적 키 구조는 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 가지고 있다 [9].

- PSK(Pre-Shared Key)

DCAS 해드앤드와 DCAS 호스트가 사전에 공유하는 키이다. 본 논문에서는 DCAS 해드앤드는 PSK를 가지고 있지 않으며 DCAS 해드앤드가 모바일 번호에 대한 키 검증자만을 가지고 있다.

- MK(Master Key)

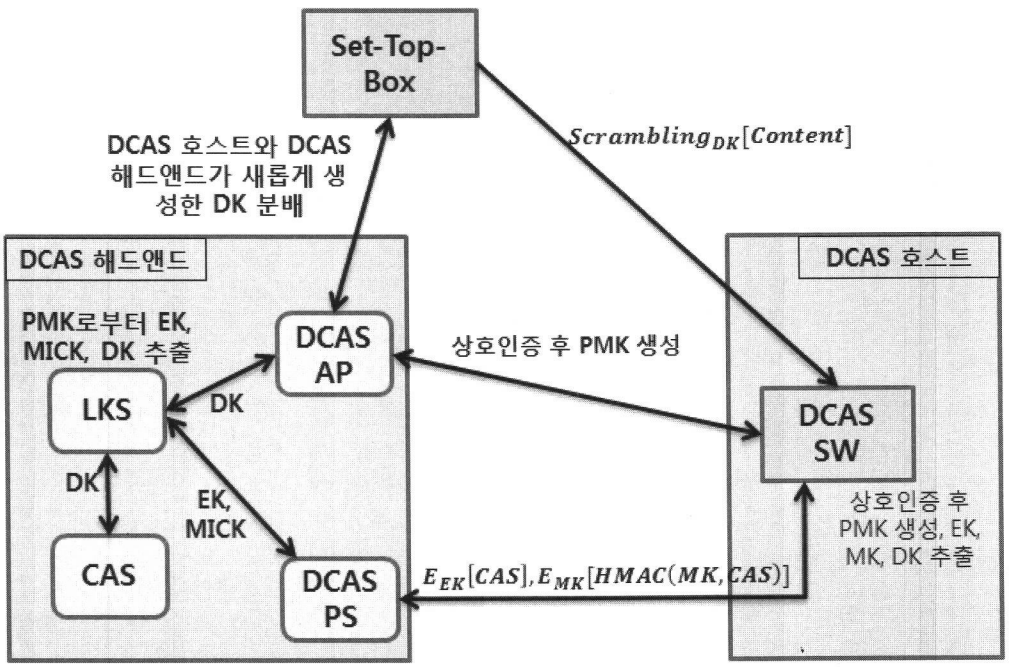
PSK로부터 PMK를 유도하기 위해 생성되는 임시키이며, AP와 모바일 호스트의 상호인증 과정에서 생성되는 세션키이다.

- 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 크기



〈그림 6〉 콘텐츠 공유를 위한 DCAS 키 분배

의 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)

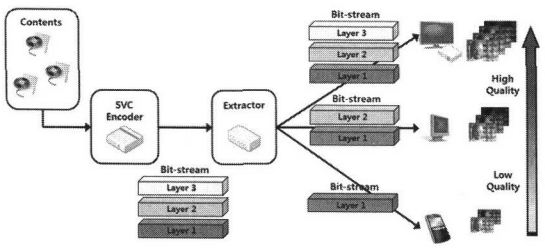
SM 클라이언트가 DCAS 호스트에 다운로드된 후, 실제 CAS의 동작에서 필요로 하는 키이다. CAS는 DK를 이용하여 콘텐츠의 스크램블링에 사용된 CW를 복호화한다. DK는 PMK로부터 특정 비트열로 추출된다.

3.3 키 교환 및 상호인증

위의 <그림 7>은 안전한 콘텐츠 공유를 가능하게 하는 DCAS 시스템을 위한 SCP 프로토콜을 사용한 키 분배를 보여준다. DCAS 호스트에서 입력한 사용자의 ID와 PW로 SCK 프로토콜 수행으로 공통된 PMK를 생성한다. 이렇게 DCAS 해드앤드와 DCAS 호스트 간 생성된 PMK에서 EK, MICK, DK를 추출한다. DCAS 해드앤드는 PMK에서 추출한 EK와 MICK를 이용하여 클라이언트의 무결성과 기밀성을 위해 사용하고 DK는 셋톱박스와 사전에 공유한 PSK를 사용하여 셋톱박스에 안전하게 분배된다. 그로 인하여 셋톱박스는 공통의 DK를 이용하여 콘텐츠를 스크램블링하여 DCAS 호스트에게 전송하면 DCAS 호스트는 PMK에서 추출한 DK를 이용하여 디스크램블링 한다.

3.4 트랜스코딩

하나의 콘텐츠를 단말의 수행 능력에 따라 저품질의 화질과 고품질의 화질로 구분하여 서비스가 가능해야 한다. 이 트랜스코딩은 ITU-T의 X.1192[12]에서 제시된 방식을 이용할 수 있다. 모바일 기기의 성능이 다르고 전송 환경이 다르기 때문에 사용자가 원하고 적절한 환경에 서비스를 제공하기 위해 필요한 기술이다. 아래의 <그림 8>은 SVC (Scalable Video Cording) 서비스의 구조를 그림으로 보여주고 있다.



〈그림 7〉 SVC 서비스 구조

네트워크 전송 효율성을 제고한 SVC를 기반으로 하는 유무선 통합의 IPTV 환경은 무선 인터페이스의 협소한 대역폭, 또는 이동용 단말기의 제한적 성능과 같은 열악한 네트워크 환경에서도 원활한 영상서비스를 제공하기에 장점을 갖는 기술이다.

V. 보안 요구사항 평가

1. 모바일 IPTV 문제점 해결

1.1 안전한 키 교환 프로토콜

본 논문에서 제안한 DCAS 보안 프레임워크에 IETF에서 드래프트로 정의된 SRP 프로토콜에 기반을 둔 DCAS 해드앤드와 DCAS 호스트 간의 키 교환 방식을 이용했. 휴대가 용이한 모바일의 특성으로 셋톱박스와 다르게 스마트카드와 같은 키 저장매체를 사용하는데 어렵고 분실의 위험성까지 존재하여 모바일에 키의 저장은 많은 위험을 가지고 있다. 하지만 SRP 프로토콜의 적용으로 사용자가 DCAS 해드앤드에 저장한 ID와 PW를 이용하여 DCAS 호스트에 저장할 필요가 없다.

또한 ITU-T의 X.1193에서 정의한 계층적 키 구조를 적용하여 DCAS 해드앤드와 DCAS 호스트간에 생성된 공통된 PMK로 MICK, EK, DK의 추출이 가능하게 되었다. 또한 클라이언트의 무결성과 기밀성을 위해 추가적으로 필요한 MICK, EK의 추출로 추가적인 키 교환이 필요 없게 되었다.

1.2 상호인증

현재 오플케이블의 DCAS 규격에서는 DCAS 서버와 DCAS 호스트가 공유키를 이용해 상호인증을 수행하도록 정의하고 있지만, 구체적인 인증 메커니즘에 대해서는 별도로 정의하고 있지 않다. 본 논문에서는 SRP 프로토콜의 적용으로 공통된 PMK를 생성 후 과정 ⑤로 DCAS 해드앤드는 DCAS 호스트를 인증할 수 있고 과정 ⑥으로 DCAS 호스트는 DCAS 해드앤드를 인증함으로써 상호인증이 가능하다.

1.3 안전한 DCAS 클라이언트 분배

오픈케이블의 DCAS 규격에서는 DCAS 서버로부터 다운로드하는 DCAS 클라이언트의 보호 방안에 대해서는 별도로 기술하고 있지 않기 때문에 ITU-T의 X.1193에서 정의한 계층적 키 구조를 적용하였다. 계층적 키의 사용으로 DCAS 해드앤드와 DCAS 호스트가 공유한 공통의 PMK로부터 MICK, EK, DK의 추가적인 키의 추출이 가능하게 되었다. MICK를 통해 클라이언트의 무결성을 확인할 수 있고 EK를 이용하여 클라이언트의 기밀성을 보장할 수 있다.

2. 보안 요구사항 분석

2.1 기존 보안 요구사항 평가

보안 요구사항 1부터 보안 요구사항 5까지는 [8]에서 정의하고 있는 DCAS 호스트 시스템에 필요한 것으로 네트워크와 관련된 보안 요구사항은 포함하고 있지 않아 본 논문에서는 다루지 않는다.

[6]에서 정의한 보안 요구사항 6부터 보안 요구사항 17까지의 내용을 간단히 살펴본다. 보안 요구사항 6과 보안 요구사항 7의 내용은 DCAS 서버와 DCAS 호스트의 상호인증에 대해서 다루는 것으로 DCAS AP와 DCAS PS가 논리적으로는 DCAS 서버에 속하는 구성요소 이지만 각각의 DCAS 호스트와 상호인증이 필요하다는 것이다. 보안 요구사항 8부터 보안 요구사항 10까지의 내용은 DCAS 서버를 구성하고 있는 구성요소 간 상호인증이 필요하다는 것이다. 보안 요구사항 11부터 보안 요구사항 13까지는 DCAS 서버의 접근제어와 관련되었다. 마지막으로 보안 요구사항 14부터 보안 요구사항 17까지의 내용은 DCAS 구성요소 간, DCAS 서버와 DCAS 호스트 간 통신보안을 다루고 있다.

보안 요구사항 6, 7 : DCAS 해드앤드와 DCAS 호스트의 상호인증에 관한 요구사항으로 SCP 프로토콜의 과정 ⑤를 통하여 DCAS 해드앤드는 DCAS 호스트를 인증하고 과정 ⑥을 통하여 DCAS 호스트가 DCAS 해드앤드를 인증하여 두 DCAS 해드앤드와 DCAS 호스트는 상호 인증이 이루어 진다.

보안 요구사항 8, 9, 10 : DCAS 해드앤드를 구성하고 있는 서버간 상호인증이 필요하여 각 서버 간에는 SSL 기반의 상호인증을 수행하도록 하여 만족하였다.

보안 요구사항 11, 12, 13 : DCAS 서버의 접근제어와 관련된 보안 요구사항으로 DCAS LKS는 TA와 AP에게만 통신을 허용하고 DPS, PS는 AP와의 통신만 허용하도록 하여 프레임워크를 구성하였다.

보안 요구사항 14, 15, 16 : DCAS AP와 DCAS LKS간, DCAS AP와 DPS, DCAS AP와 DCAS PS간 통신은 SSL을 통하여 보호하도록 하였다.

보안 요구사항 17 : DCAS PS와 DCAS 호스트간 통신 내용은 DCAS PS와 DCAS 호스트가 상호인증 과정에서 분배한 PMK를 통해서 보호된다.

2.2 추가 보안 요구사항 평가

위에서 정의한 보안 요구사항에 본 논문에서 제안한 안전한 콘텐츠 공유를 위한 모바일 IPTV 환경의 DCAS 보안 프레임워크에서 추가적으로 요구되는 보안 사항을 정의하였다. 기존의 보안 요구사항들에서는 본 논문에서 제안한 안전한 콘텐츠 공유를 위한 모바일 IPTV환경의 DCAS 시스템의 보안을 만족하는데 한계가 따른다. 먼저 DCAS 해드앤드에 콘텐츠가 저장되지 않고 사용자가 직접 자신의 저장소에 콘텐츠를 저장하고 DCAS 시스템의 제공만을 해드앤드에 의존하는 형태에서 새롭게 요구되는 보안을 제시하였다. 또한 모바일 IPTV의 환경에 맞는 이동성과 휴대성, 보관성을 고려한 보안 요구사항이 필요하다. 이러한 배경에 제 3장에서 문제점과 보안 요구사항을 분석하고 제시하였다. 다음은 위에서 제시한 보안 요구사항 18부터 보안 요구사항 22까지의 내용을 본 논문에서 제안한 보안 프레임워크를 평가한 내용이다.

보안 요구사항 18: DCAS AP와 DCAS 호스트 간 PSK는 오픈케이블에서 정의한 PSK와 KD와 같은 키 정보를 사전에 미리 스마트카드와 같은 다른 물리적 수단으로 DCAS 호스트와 DCAS 해드앤드가 사전에 공유한다. 하지만 본 논문에서 적용한 SCP 프로토콜을 통하여 사전에 등록한 ID와 PW를 이용하여 DCAS 호스트에서는 저장되어있는 키정보를 사용하지 않고 사용자의 ID와 PW를 사용하여 PMK를 생성할 수 있다.

보안 요구사항 19: 현재의 오픈케이블 DCAS 규정에서 사용중인 PSK와 DK 정보는 모바일 기기에 저장되지 않는다. 사전에 미리 DCAS 해드앤드에 사용자의

ID와 PW를 저장하여 DCAS 호스트에서는 물리적으로 키를 저장하고 있지 않을 수 있다.

보안 요구사항 20: 셋톱박스와 DCAS 해드앤드 간 DK는 셋톱박스와 DCAS 해드앤드가 사전에 공유한 PSK를 사용하여 안전하게 통신이 가능하다. 셋톱박스와 DCAS 해드앤드 간에 스마트카드와 같은 물리적 저장매체를 사용하여 사전에 안전한 키의 공유가 가능하다.

보안 요구사항 21: DCAS 호스트와 DCAS 해드앤드 간 DK는 둘 간의 SCP 프로토콜을 통하여 생성한 공통의 PMK를 통하여 가능하다. 계층적 키 구조의 특징으로 PMK에서 DK의 추출이 가능하여 DCAS 호스트는 DCAS 해드앤드와 안전하게 DK를 소유할 수 있다.

보안 요구사항 22: 보안 요구사항 20과 보안 요구사항 21의 만족으로 DCAS 호스트와 셋톱박스는 공통의 DK를 가지게 된다. 그로 인하여 DK로 스크램블링된 콘텐츠는 안전하게 DCAS 호스트에게 전송할 수 있다.

Ⅵ. 결 론

기존의 IPTV는 이동성과 휴대성이 가능한 모바일 IPTV로의 확장이 요구되고 있다. 최근 스마트폰 시장의 급성장은 향후 모바일 IPTV의 활성화에 더욱 박차를 가하게 해주는 계기가 될 것이며 미래의 방송통신에 큰 영향을 미칠 것으로 예상된다. 기존의 IPTV 사용자는 셋톱박스를 통하여 시청하던 콘텐츠를 다른 모바일 기기로의 확장까지 원하고 있다. 자신이 소유한 콘텐츠를 원하는 곳에서 안전하고 편리하게 시청할 수 있는 것이 필요하다.

본 논문에서는 모바일 IPTV 환경에서의 안전한 콘텐츠 공유를 위한 DCAS 보안 프레임워크를 제안하였다. 모바일 IPTV가 가지는 보안 문제점을 분석하고 현재 오픈케이블에서 진행중이 DCAS의 보안 문제점을 분석하여 본 논문에서 제안한 보안 프레임워크에서 요구하는 보안사항을 정리하고 추가로 제시하였다. 위에서 분석한 보안 문제점과 보안 요구사항을 만족하기 위해 모바일 IPTV의 환경을 고려한 안전한 키 교환 프로토콜로 표준으로 제정된 SRP 프로토콜과 계층적 키 구조를 사용하였다. 또한 우수한 호환성, 간단하고 편리한 클라이언트의 업데이트, 다른 서비스와의 우수한 연동성 등의 장점이 있는 DCAS를 기반으로 제안하였다.

모바일 IPTV에 DCAS를 적용하기 위해서 발생 가능한 모든 보안 문제점에 대해서 연구하고 보안 모델을 수립할 필요가 있다. 본 논문의 결과는 오픈케이블의 DCAS의 활발한 연구 및 표준화의 기반을 제공하며, ITU-T IPTV 키관리와 암호알고리즘 등의 국제적인 IPTV 보안 표준화에 활용되어질 수 있다.

참고문헌

[1] KBS 방송기술연구 2007, "DTV 콘텐츠 저작권 보호 기술 및 동향," KBS, 2007년.

[2] TTA Standard, "IPTV 용 교환 가능한 CAS (iCAS)," TTAK.KO-08.0023, 2010-03-26.

[3] 김영일, 조철회, 류원, 이호진, "모바일 IPTV 기술 현황 및 연구 추진 방향," 전자통신동향분석 제25권 제2호, 2010년 4월.

[4] 서창호, 박종열, 문진영, 백의현, "IPTV 접근제어 표준 및 서비스 기술," TTA Journal, 110호, 2007년 4월.

[5] 박지헌, 정연정, 윤기송, "DRM 기술 동향," 전자통신동향분석, 제22권 제4호, pp. 118-132, 2007년 8월.

[6] 강성구, "안전한 다운로드 가능 제한 수신 시스템 제안 및 구현," 한국정보보호학회지, 제19권 제6호, pp. 165-166, 2009년 12월.

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

[8] OpenCable, "OC-SP-CKL2.0-106-080118: Common Download 2.0," OpenCable Specification, Jan. 2008.

[9] ITU-T X.1193, "Key management framework for secure IPTV services for consent," 2011.

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

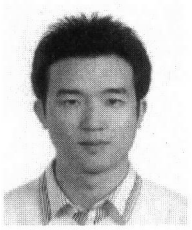
[11] ITUT2011, "Functional requirements and mechanisms for the secure transcodable scheme of IPTV," ITU-T X.1192, 2011.

[12] M. Pagani, Multimedia and Ineractive Digital TV: Managing the Opportunities Created by Digital Convergence, IRM Press, Apr. 2003.

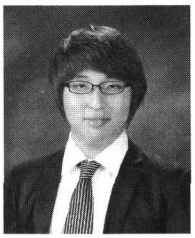
[13] 최종연구보고서, "디지털 방송용 RMP 기반 기술

연구", 한국전자통신연구원, 2002년 10월.
[14] 최현우, "OTP 기반 IPTV 콘텐츠 보호 및 인증 시스템," 순천향대학교, 2010년 12월.
[15] Ken Kerpez, Dave Waring, George Lapiotis, J. Bryan Lyles, and Ravi Vaidyanathan, "IPTV Service Assurance," IEEE Communications Magazine, vol. 44, no. 9, pp. 166-72, Sep. 2006
[16] K. Kerpez. "IPTV service assurance," IEEE Communications Magazine. vol. 44, no. 9, pp. 166-172, Sep. 2006.
[17] 이승엽, 박상현, 김경미, "DMB2.0 서비스", 한국방송공학회지 제14권 제1호, pp. 17-25, 2009년 3월
[18] 장지원, 김영한, "DVB-H 네트워크에서 PMIPv6 기반 이동성 관리", 정보과학회논문지 제38권 제3호, pp.191-197, 2011년 6월
[19] 최인환, 송재형, 서종열, "ATSC-M/H 기술 소개", 한국방송공학회지 제14권 제1호, pp. 31-52, 2009년 3월

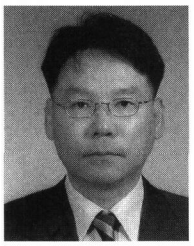
〈著者紹介〉



정 영 곤 (Young-gon, JUNG)
학생회원
2010년 2월 : 순천향대학교 정보보호학과 졸업
2010년 3월 ~ 현재 : 순천향대학교 정보보호학과 석사과정
관심분야 : IPTV 보안, 정보보호, 인증프로토콜



조 효 제 (Hyo-Je Jo)
학생회원
2011년 2월 : 순천향대학교 정보보호학과 졸업
2011년 3월~현재 : 순천향대학교 정보보호학과 석사과정
관심분야 : 정보보호



염 흥 열(Heung-Youl YOUM)
종신회원
1981년 2월 : 한양대학교 전자공학과 학사 졸업
1983년 2월 : 한양대학교 대학원 전자공학과 석사 졸업
1990년 2월 : 한양대학교 대학원 전자공학과 박사 졸업
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, 수석부회장(역), 학회장(역), 명예회장
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 (구) 정통부 정보보호 PM/정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜