情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

모바일 IPTV 환경에 적합한 DCAS 보안 프레임워크 연구

최 중 영,† 조 관 태, 임 종 인‡
고려대학교 정보경영공학전문대학원

A Study on DCAS Security Framework Model for Mobile IPTV

Jung-Young Choi,† Kwan-tae Cho, Jong-in Lim‡
Graduate School of Information Management and Security, Korea University

요 약

모바일 IPTV는 무선 인터넷 망을 이용하여 IPTV의 양방향 서비스에 이동성을 함께 제공함으로써 사용자의 편의를 증대시킬 수 있는 기술이다. 이러한 모바일 IPTV 서비스는 더욱 많은 수요를 불러올 것으로 예상되는데, 성공적인 사업화와 서비스 활성화를 위해서는 무선 환경과 모바일 통신단말기를 이용한 콘텐츠 보호 등 다양한 기술적 이슈를 해결해야 한다. 본 논문에서는 모바일 IPTV 특성과 모바일 IPTV 서비스를 위한 보안 요구사항을 살펴보고, 그에 따라 요구되는 콘텐츠 보안의 문제점들을 살펴보고자 한다. 또한 이를 해결하기 위한 모바일 IPTV환경에서 DCAS 보안 프레임워크 모델을 제시하고, 기존 DCAS에 비하여 개선된 사항을 평가한다.

ABSTRACT

Mobile IPTV is a IPTV interactive broadcasting service through wireless Internet. Mobile IPTV service would be much more promoted. Thus, the methods for protecting the broadcasting contents will be indispensible elements for the successful Mobile IPTV service achievement. This paper describes the characteristics of Mobile IPTV and the related contents protection techniques. To evaluate several security issues, we suggest a DCAS security framework model for Mobile IPTV, and speculate the most widespread, a security technologies for Mobile IPTV such as DCSA. Moreover, candidate models of Mobile IPTV protection system are suggested based on these technologies.

Keywords: Mobile IPTV, DCAS

I. 서 론

세계적으로 IPTV의 서비스를 상용화 했거나 도입을 준비 중인 나라가 늘어나고 있다. 주요 선진국에서는 통신 사업자들의 IPTV 시장 진입을 허용하였고, 진입 규제를 완화하여 각국의 정보통신산업의 신성장 동력으로 추진하고 있다. 우리나라도 '인터넷 멀티미디어 방송사업법' 및 하위법령들의 제정 및 시행으로 2009년부터 실질적인 IPTV 서비스가 시작되었다. 또한 광대역 통합망(BcN) 환경이 구축되는 시점을 기준으로 IPTV 서비스는 더욱 많은 수요를 불러올 것을 예상된다. 특히 아이폰의 국내발매로 시작된 스마트폰의 급성장은 향후 모바일 IPTV의 활성화에 더욱 박차를 가하는 계기가 될 것이다.

모바일 IPTV 상용 서비스가 시작됨에 따라 성공적인 사업화와 서비스 활성화를 위하여 경쟁력 있는 콘텐츠 확보와 콘텐츠의 안전한 유통 및 저작권 보호 방안이 중요시된다. 단방향으로 서비스되던 기존 방송의 방송망과 달리, 모바일 IPTV는 특성상 IP주소만 있으면 장소와 시간의 제약에서 벗어나 다양한 콘텐츠를

접수일(2010년 6월 30일), 수정일(2010년 11월 14일)
게재확정일(2011년 1월 10일)
† 주저자, billy-choi@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

제공받을 수 있는 특징이 있다.

고정형 IPTV와 달리 Mobile IPTV의 서비스 제공을 위해 물리적 제약(Low Network Reliability(QoS), Low Device Capability 등)으로부터 사용자 요구 사항을 충족시킬수 있는 기술이 개발되어야 하며 모바일이 갖는 특성과 IPTV 서비스의 특성을 콘텐츠 사용자 및 제공자 관점에서 접목시킨 새로운 서비스 기술과 그에 따른 보안 기술 개발되어야 한다. 본 논문에서는 모바일 IPTV 서비스에 필요한 보안 모델을 DCAS 중심으로 제시하고, 그에 대한 근본적인 해결 방안을 모색하고자 한다. 기존 OpenCable 기반의 DCAS 시스템을 모바일 IPTV 기반의 DCAS 시스템으로 전환 시 발생 가능한 보안 문제점에 대해서 점검하고 이를 해결하기 위해 필요한 보안 프레임워크를 제안한다. 그러한 보안 프레임워크를 운용하기 위해 필요한 보안 요구사항을 도출하고, 이러한 보안 요구사항을 만족시킬 수 있는 모바일 IPTV에서의 안전한 DCAS 보안 프레임워크를 제안한다.

논문의 구성은 다음과 같다. 2장에서는 모바일 IPTV 특성과 문제점을 분석하고, 3장에서는 보안기술을 소개하고 장단점을 평가해본다. 4장에서는 모바일 IPTV 보호 시스템의 구현 모델에 대하여 제안하고, 마지막으로 5장에서는 결론을 맺는다.

II. 모바일 IPTV

2.1 모바일 IPTV 개요

모바일 IPTV는 기존 IPTV 기술에 무선기술과 이동성기술을 확장한 형태의 새로운 서비스로 무선구간에서 이동성을 지원하여 언제, 어디서나, 자유롭게 IPTV를 이용하도록 하는 서비스로 정의하고 있다[1]. 이는 유무선 융합이나 방통융합의 개념을 담아서, 다양한 서비스간의 융합으로 개인화, 양방향 통신, 이동성 등을 제공 할 수 있음을 뜻한다. 이에 IPTV사업자들은 사용자에게 새롭고 다양한 서비스 제공을 위해 서비스 발굴에 박차를 가하는 반면, 사용자는 장소와 단말종류에 제약 없이 언제, 어디서나 최적의 품질로 끊임없는 서비스를 제공받기를 원하고 있다.

모바일 IPTV가 도입되면 맞춤형 TV앨범·UCC, 참여형 교통방송·연동형 영화·드라마 같은 양방향 서비스도 가능해 진다. 또한 유·무선 네트워크에 상관없이 가정에서 IPTV를 보다가 외출할 일이 생기면 휴대 단말기를 통해 계속 시청할 수 있는 Take-Out TV(Mobile IPTV-DMB, DVB, MediaFLO) 서비스가 가능해진다.

2.2 모바일 IPTV 서비스 제공 기술

모바일 IPTV 기술은 모바일 TV의 확장, 고정형 IPTV의 확장, 그리고 이동통신 상의 멀티미디어 서비스의 확장으로 나누어 볼 수 있다.

2.2.1 모바일 TV의 확장

지상파/위성 DMB, DVB-H, MediaFLO 등 현재 제공 중인 모바일 TV는 단방향 서비스로 IP기술을 기반으로 개발되지 않았다. 하지만 IP를 기반으로 하여 인터넷 상의 다양한 콘텐츠와 인터넷 기술의 장점을 모바일 TV 사용자에게 전달하기 위하여 IP 기술의 융합이 개발되고 있다. 이와 같은 모바일 TV와 IP를 결합한 형태의 모바일 IPTV 서비스는 디지털 방송 네트워크를 사용하여 IP 기반의 오디오/비디오/데이터 등을 사용자에게 전달하는 방식이다[2]. 현재 개발 중인 방식은 기존 모바일 TV에 리턴 채널을 결합하여 양방향 서비스로 확장하는 형태이며, 최근 국내에서는 리턴 채널을 위한 기술로 WiBro를 접목한 양방향 형태의 모바일 IPTV 기술 개발을 시도하고 있다[3]. 유럽의 DVB-H는 유럽 전역에 서비스가 가능한 3GPP(3rd Generation Partnership Project)의 무선 규격을 리턴 채널로 사용하여 양방향 모바일 TV 기술 개발을 진행하고 있다.

2.2.2 고정형 IPTV의 확장

고정형 IPTV는 인터넷의 다양한 콘텐츠를 IP망을 통해 사용자에게 전송하는 방식이며 모바일 IPTV는 고정형 IPTV를 무선에서 구현하는 방식이다. 무선 기술은 제한 없이 모든 기술이 사용될 수 있으며, 최근 국내에서는 Wibro, 해외에서는 광대역 무선접속 기술인 WiMAX(Worldwide Interoperability for Microwave Access)를 이용하여 IPTV 기술이 개발되고 있다[4]. 특히 IPTV서비스와 같은 멀티미디어 콘텐츠를 해당 무선 기술상에서 보다 효율적으로 전달하기 위해 무선 기술을 확장하고 있는데 즉, WiBro의 기반 기술인 IEEE 802.16e에서는 MBS

(Multicast Broadcast Service)에 대한 전송 방식에 대한 표준이 추가 되었다.

2.2.3 이동통신영역에서의 모바일 IPTV

이동통신 사업자가 제공하는 멀티미디어 서비스 역시 초기 모바일 IPTV 서비스로 볼 수 있다. 이동통신 영역에서 IPTV 서비스를 제공하기 위해 연구되고 있는 가장 대표적인 기술은 OMA BCAST(Broad-CAST) 으로 다양한 모바일 통신 단말들이 IPTV와 같은 형태의 서비스들을 원활하게 수신할 수 있도록 한다[5].

이와 같이 모바일 IPTV는 사용자가 무선랜과 와이브로망, 무선랜과 CDMA 망간의 자유로운 이동처럼 이기종간의 멀티미디어 서비스를 사용할 수 있도록 지원하는 기술 개발이 중요하다. 서비스 연속성 보장 기술인 핸드오버가 그 대표적인 기술로 볼 수 있으며, 이를 통해 사용자는 다른 무선접속 구간으로 이동할 때도 끊김없는 방송 서비스를 제공받을 수 있다[6].

2.3 모바일 IPTV 보안 문제점 고찰

Mobile IPTV 서비스 역시 기존 IPTV 서비스와 마찬가지로 유선망 Telco 진영, 이동통신사업자 진영, 케이블/DTV 진영 그리고 기존 인터넷 사업자 진영 등이 서로 경합을 벌일 것으로 예측되고 있어, 만일 기존의 IPTV 콘텐츠를 단순히 모바일 단말로 제공하는 서비스의 형태가 된다면 기존 경쟁자와의 차별성을 극복하지 못하고 결국 실패할 확률이 높다고 할 수 있다. Mobile IPTV 서비스 제공을 위해 선결되어야 할 여러 가지 물리적 제약(Low Network Reliability(QoS), Low Device Capability 등) 만큼이나 또는 그 이상으로 중요한 것은 모바일이 갖는 특성과 IPTV 서비스의 특성을 철저히 콘텐츠 사용자 및 제공자 관점에서 접목시킨 새로운 서비스 기술과 그에 따른 보호 기술이라고 할 수 있다.

2.3.1 무선 환경에서의 문제점

Wi-Fi는 기존의 이더넷의 단점인 케이블을 제거하여 Local Area에서 별도의 배선 작업 없이 AP를 통해 외부망으로 나가는 장점이 있다. 따라서 Wi-Fi를 사용하기 위해서는 넓은 무선 구간을 확보해야 하고, 이러한 무선 구간을 확보하기 위해서는 많은 비용이 소모된다. 이미 국내의 무선 인프라는 잘 구축되어 있는 상태지만, 모바일 단말기 같은 이동성이 잦은 개체들을 지원하기 위해서는 아직 인프라가 많이 부족한 실정이다.

특히 기존의 이동통신사를 경유하여 여러 콘텐츠 제공서버에 접근하던 모바일 단말기의 경우 Wi-Fi환경에서 직접적으로 콘텐츠 제공서버에 접근함으로써 다음과 같은 문제를 야기한다.

2.3.2 콘텐츠 제공 서버 인증

기존의 모바일 단말기가 이동통신사를 경유하여 콘텐츠 제공서버에 접근하면 콘텐츠 제공 서버에서 단말기로 유입되는 데이터를 이동통신사가 필터링하여 악성코드의 유입을 막고, 단말기가 인증되지 않은 콘텐츠 제공 서버에 접근하는 것을 제어할 수 있었다. 하지만 Wi-Fi환경에서는 모바일 단말기는 이동통신사로부터 보안 메커니즘을 제공받지 못하기 때문에 인증되지 않은 악의적 사이트로부터 유입되는 악성코드, 트로이 목마, 바이러스 등을 통해 제공받은 콘텐츠의 신뢰성을 보장하기가 어렵다.

2.3.3 사용자 인증

콘텐츠 제공 서버 역시 이동통신사의 신뢰할 수 있는 단말기 인증 메커니즘을 제공받지 못하기 때문에 정당한 사용자로 위장한 가장 공격에 노출될 수 있으며, 이러한 공격을 통하여 콘텐츠 제공서버의 지적자산인 콘텐츠를 악의적인 사용자에게 갈취 당할 수 있다. 또한 콘텐츠 사용자가 제공받은 사실에 대한 부인을 봉쇄할 수 있는 메커니즘이 없다.

2.3.4 모바일 IPTV 단말기의 제약

모바일 IPTV 단말은 스마트폰 및 휴대폰이나 PDA와 같이 통신 서비스를 제공하는 작은 크기의 휴대용 컴퓨터이다. 초기의 휴대용 통신 단말은 휴대용 전화기와 같이 단순한 하나의 통신 서비스를 제공하는 수준이었다. 그러나 현재는 CDMA, Bluetooth, WiFi, Wibro 등과 같은 이종의 통신장치를 지원하는 멀티통신 서비스와 IPTV, DMB(Digital Multimedia Boradcasting) 등과 같은 다양한 멀티미디어 서비스를 모두 통합하여 하나의 단말에서 제공할 수 있도록 진화하고 있다. 모바일 단말의 특징은 아래와 같다.

모바일 단말의 특징

- 불편한 사용자 인터페이스: 스크린이 작고 키보드를 통한 입력이 불편함
- 배터리 사용
- 저성능 컴퓨팅 자원: CPU, 메모리 등 컴퓨팅 성능이 제한적임
- 멀티 통신 장치: USB, Bluetooth, WiFi, CDMA 등 다양한 통신 장치를 제공함
- 통합 단말: 네비게이션, DMB, 카메라, MP3플레이어 등의 서비스를 하나의 단말에서 제공함

위와 같이 상대적으로 느린 연산 처리 속도, 적은 저장 공간 같은 모바일 단말기의 제한된 환경 문제로 인하여 기존의 유선망에서 적용되던 IPTV 기반의 보안기술의 활용하는데 제약이 있다.

III. 보안 기술

모바일 IPTV의 보안을 위해 사용되는 기술은 적법한 수신자를 가려내는 CAS(Conditional Access System)과 콘텐츠 보호를 위한 DRM(Digital Right Management) 등이 있다. CAS는 유료방송 서비스에 사용하는 시스템으로 암호화를 수행하여 인증된 사용자에게 채널 및 콘텐츠를 이용할 수 있도록 제어하는 방법이며 다양한 비즈니스 모델에 적용할 수 있을 뿐만 아니라 보안성이 우수하다. DRM은 암호화 기술로 불법복제 및 유통을 방지하는 기술로 솔루션 비용이 저가이지만 보안성이 취약하다.

3.1 Conditional Access System(CAS)

CAS 솔루션은 시청권한이 있는 사용자에게만 콘텐츠 서비스에 대한 접근을 허용하는 기술로서, 방송신호를 암호화하여 송출하고 유료서비스에 가입한 사람의 수신 장치에서 암호화된 방송신호를 풀 수 있는 복호키를 전송하여 방송 콘텐츠 수신자격을 부여한다[7]. KBS, MBC 등 지상파 TV 방송사에서 헤드엔드(Headend, 모바일 IPTV 서비스 운영센터)로 전송된 실시간 방송 신호를 전송 및 저장 효율을 높이기 위해 인코더(H.264 등)로 인코딩(압축)한다. 인코딩된 모바일 IPTV 신호는 스크램블러(scrambler)에 의해 암호화된 후 방송채널로 보내면 모바일 인터넷 멀티캐스트 망을 통하여 모바일 단말기로 전달된다. 스크램블러가 사용하는 암호화 알고리즘은 CAS(Common Scrambling Algorithm)와 AES(Advanced Encryption Standard) 등이 있다.

스크램블러가 채널 암호화에 사용하는 키는 제어단어(Control Word: CW)라고 하며, CW생성기(CWG, CW Generator)에 의해 생성된다. CW는 모바일 단말기에 채널 복호화 과정에서도 사용되기 때문에, CW를 서비스 키(Service Key)로 암호화하여 ECM(Entitlement Control Message: 자격 제어 메시지)에 넣은 후 모바일 인터넷 망을 이용하여 사용자 단말기로 전송한다. ECM은 통상 채널 혹은 방송 프로그램마다 별도로 생성되며, 초 단위 주기로 갱신되어 전송되는 데 통상 10초 주기를 많이 사용한다. 채널 시청 권한을 담고 있는 수신 자격(Entitlement)에는 CW 의 암호화에 사용된 서비스키, 가입자 고유 식별정보, 가입자의 각 방송프로그램에 대한 수신 자격은 EMM (Entitlement Management Message, 자격 관리 메시지)를 이용하여 사용자 단말기에 전달된다. EMM 는 가입자 정보 변경시(프로그램 구매 등)또는 월 단위로 발급되며, EMM 의 주요정보는 단말기의 스마트 카드에 저장된다. 헤드엔드(Headend)의 다중화 장치(MUX, Multiplexer)는 스크램블 된 여러 개의 방송 신호와 ECM, EMM 등을 역다중화 장치(DeMUX)를 분리하여 디스크램블러(descrambler)와 스마트카드로 각각 전송한다. 스마트 카드에서는 EMM 의 가입자 식별정도(Address)를 이용하여 자신에게 전달된 EMM 인지를 판단하고, 스마트카드에 들어있는 사용자키(User Key)를 이용하여 EMM에 들어있는 서비스 키를 추출하고, 서비스키로 ECM에서 CW를 추출한 다음에 이를 디스크램블러로 전달한다. 디스크램블러는 CW를 이용하여 스크램블러된 방송 신호를 복호화하여 단말기에 있는 디코더 등에 전달하면, 디코더는 압축된 방송스트림을 복원하여 모바일 단말기의 디스플레이와 오디오 출력단자로 전송한다[8].

3.2 Digital Right Management(DRM)

DRM은 암복호화 기술, 콘텐츠 사용권한, 그리고 사용자 인증 등을 이용하여 모바일 디지털 콘텐츠를 보호하는 방법이다. DRM 시스템은 콘텐츠를 암호화하는 DRM 패키저(Packager), DRM 라이센스(복호화키와 사용권한 포함)를 발급하는 DRM 서버, 그리고 DRM 에이전트(Agent)로 이루어진다. DRM 패키저는 통산 AES(Advanced Encryption

〔표 1〕 국내외 모바일 콘텐츠서비스 및 보호 솔루션[10]

서비스명	개요	사용
iTunesStore(Apple)	온라인 음악/비디오 제공서비스	- 유료다운로드:FairPlay DRM 사용 - DRM free MP3판매
Rhapsody(RealNetworks와 MTV Networks의 합작 온라인 음악사업)	- Verizon 무선망을 이용한 무선 다운로드 서비스 - 유선은 DRM-free MP3유료다운로드서비스와 월정액 주문형스트리밍서비스의 결합	MS Windows Media DRM
PlayNow	Sony Ericsson의 유럽모바일 음악서비스 Denmark, Finland, Norway and Sweden	DRM free
Ovi(노키아)	Music Store, N-Gage게임서비스와 노키아 Map 등의 통합서비스	Window Media DRM사용
MotoMusic(모토롤라)	싱가폴 소재 SoundBuzz가 제공하는 음악, 비디오, 링톤의 다운로드 서비스	음악은 Windows Media DRM 사용
멜론(낫)	휴대폰 오디오 서비스	SKT DRM(OMA 2.0)
도시락(KTF)	휴대폰 오디오 서비스	KTF DRM(OMA 2.0)
MusicOn(LGT)	휴대폰 오디오 서비스	LGT DRM
Mobile TV 서비스	- Cingular/AT&T가 제공 - Qualcomm의 MediaFLO플랫폼을 사용한 모바일 IPTV 서비스	CAS 기술 혹은 모바일 DRM 기술 사용
	- Spain소재 Abertis Telecom에서 제공 - DVB-H 기술 사용	Nagravision CAS 사용
	- V0dafone(이탈리아)이 제공 - DVB-H 기술 사용	

Standard) 128bit 암호화 알고리즘을 이용하여 디지털 콘텐츠를 암호화 한다. 콘텐츠 서비스 제공업체는 DRM 패키저로 암호화한 콘텐츠를 헤드엔드 콘텐츠 서버에 업로드 한다[9].

사용자가 디지털콘텐츠를 구매하면 통합관리시스템은 모바일 장치의 고유정보를 이용하여 사용자 인증을 거친 다음에 사용자의 지불 사실이 확인되면, DRM 라이센스를 암호화하여 사용자에게 전달한다. 모바일 단말기의 DRM 에이전트는 DRM 라이센스에 포함되어 있는 복호키를 추출하여 암호화된 콘텐츠를 복호화하고 콘텐츠 사용권한에 따라 콘텐츠 사용을 제어한다.

DRM 라이센스를 적합한 사용자에게 전달하는 방식으로 PK(Public Key) 시스템을 이용한다. PK시스템이란 DRM 라이센스 서버와 모바일 단말기에서 각각 공개키(Public Key)와 개인키(Private Key), 쌍키(Pairwise Key)를 만들어 통합관리시스템의 DRM 서버와 모바일 단말기에 각각 저장한다. DRM 서버가 모바일 단말기에게 라이센스를 발급할 경우에는 모바일 단말기의 공개키를 이용하여 라이센스를 암호화해서 보내면, 모바일 단말기는 자신의 개인키를 이용하여 라이센스를 복호화 한다. PK시스템을 이용함으로써 특정 모바일 단말기에게만 동작 가능한 라이센스를 전송할 수 있다.

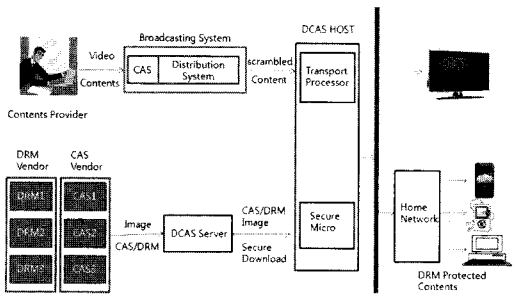
3.3 DCAS(Downloadable Conditional Access System)

Downloadable Conditional Access System의 약자인 DCAS는 제한수신 시스템(CAS)의 일종으로, 가입자의 셋톱박스(STB)나 일체형 TV에 하드웨어 형태의 제한수신 모듈을 별도로 두지 않고, 사업자가 소프트웨어 제한수신 시스템을 가입자 단말에 바로 다운로드 시켜 유료 방송을 시청할 수 있도록 하는 수신 인증기술이다. DCAS 기술은 STB에 제한수신 모듈(CAS)이 미리 설치되어 있는 것이 아니라, STB에서 네트워크 연결을 시도할 때 DCAS Server로부터 CAS Image를 안전하게 DCAS HOST의 SM에 다운로드하여 설치한 후 스크램블 된 방송을 디스크램블 하여 시청할 수 있도록 하는 기술이다. 이는 다운로드 받은 CAS, DRM, ASD(Authorized Service Domain) 등의 콘텐츠 보호 모듈이 잘 구동되어 서비스 될 수 있도록 지원하는 플랫폼 기술이다.

유료 방송 시스템에서 DCAS가 적용될 경우에는

현재 CAS에서 디지털 컨텐츠를 보호하기 위해서 필요한 셋톱박스(set-top box)나 케이블카드가 필요없게 된다. 바꿔 말하면 DCAS의 가장 큰 목적 가운데 하나는 디지털 TV, DVR(Digital Video Recorder), 셋톱박스 같은 OCAP 호환 장치에서 DRM등의 추가적인 보안 모듈 기술을 소프트웨어적으로 구현하는 것이라고 할 수 있다. 또한 DCAS가 적용될 경우 얻을 수 있는 또 하나의 장점은 안전성의 향상이다. 예를 들어 어떤 암호화 알고리즘이 침해되는 경우가 발생할 경우, DCAS 기술을 통해서 알고리즘의 대체가 빠르고 효율적으로 이루어질 수 있다. 즉, 기존에는 이와 같은 문제가 발생할 경우에는 하드웨어의 교체가 불가피하지만, DCAS가 적용된다면 소프트웨어의 업데이트만으로 문제의 해결이 가능하게 된다. 이와 같은 특징으로 인해 모바일 IPTV에 서비스 보안 적용 기술로 모바일 환경과 모바일 단말 제약을 고려한다면 DCAS 시스템이 적합할 것으로 생각한다[11]. 단방향 네트워크에서의 제한수신 시스템은 사용자와 동일시되는 스마트카드 또는 케이블카드가 없으면 실체 인증이 불가능하였으나 IPTV와 같이 양방향 방송이 가시화되고 있는 현재는 스마트카드와 같은 하드웨어를 통한 실체 인증이 반드시 필요하지 않게 되었기 때문이다. 또한 모바일 환경에서는 스마트카드를 읽을 수 있는 별도의 장치를 구비하는 것이 어렵기 때문에 스마트카드를 이용한 인증방법은 용이하지가 않다.

DCAS 시스템은 크게 3가지로 구성되며 DCAS 서버, DCAS HOST, 그리고 3rd party에서 SM (Secure Micro), TP(Transport Processor) 인증서를 관리하는 TA로 분류할 수 있다. DCAS 서버는 AP(Authentication Proxy), LKS(Local Key Server), PS(Personalization Server), DPS(DCAS Provisioning Server) 등의 4개의 주요 서버들로 구성되며, 각 서버들의 핵심기능들은 다음과 같다. [그림 1]은 DCAS 시스템 구성도이다.



[그림 1] DCAS 시스템 구성도[12]

3.3.1 DCAS 구성요소

DCAS 시스템은 크게 3가지로 구성되며 DCAS Server, DCAS HOST, 그리고 3rd party에서 SM(Secure Micro), TP(Transport Processor) 인증서를 관리하는 TA로 분류할 수 있다.

3.3.1.1 DCAS 서버

DCAS 서버는 AP(Authentication Proxy), LKS(Local Key Server), PS(Personalization Server), DPS(DCAS Provisioning Server) 등의 4개의 주요 서버들로 구성되며, 각 서버들의 핵심기능들은 다음과 같다.

3.3.1.1.1 AP(Authentication Proxy)

AP는 SM Client Image(CAS, DRM, ASD Client)를 DCAS 호스트내 SM으로 다운로드하기 위해 SM을 인증하고 SM과 AP간 보안통신을 구성하는 역할을 한다. SM과 보안통신을 구성 할 때 TA로부터 SM 인증을 위한 각종 인자 값들을 수신 할 뿐만 아니라 SM이 보내온 인증 정보를 TA를 통하여 확인하는 기능도 수행한다. 즉 AP는 SM들은 인증하는 서버를 의미하며, SM에 저장된 수집 정보 및 로그 정보 요청 처리를 위한 DCAS server의 Proxy 기능을 수행한다.

3.3.1.1.2 LKS (Local Key Server)

LKS는 MSO 네트워크에 대한 키 정보와 ID 정보 저장, MSO에 대한 AP 키와 ID 정보저장의 기능을 수행한다. LKS는 사업자의 네트워크에 속한 모든 SM. TP 에 대한 인증정보를 TA를 통하여 전송받고, 이미지 암호화키를 관리한다.

3.3.1.1.3 PS (Personalization Server)

DCAS 개인화 서버는 DPS의 정책에 따라 CA, DRM, ASD에 SM 클라이언트 이미지를 제공하며, 다운로드서버(Carousel, TFTP, HTTP 등)에 전달하는 기능을 담당한다. SM 클라이언트의 배포, 다운로드 관리의 근원이 되는 구성요소이다

3.3.1.1.4 DPS (DCAS Provisioning Server)

DPS는 SM 설정을 관리하며, SM Client 이미지 등록과 SM Client 이미지 관리, AP에게 DCAS 다운로드 정책 정보 등록에 의하여 이미지 다운로드에 대한 DCAS 정책 배포 와 DCAS 정책의 결정 및 유지하는 역할을 한다.

3.3.1.2 DCAS HOST

DCAS HOST는 DCAS 서비스를 지원하는 단말로 케이블방송 시스템에서 제공하는 방송신호 및 데이

터 신호를 수신하는 기능을 지닌 SM, TP구조를 갖는다. TP는 다수의 디스크램블러를 지원하는 유연화 복호화엔진을 구비해야 한다. SM은 DCAS HOST에 내장되는 보안칩으로 DCAS Server와 통신하여 SM Client Image를 설치하고, TP와 통신하여 설치된 콘텐츠 보호서비스를 제공한다.

3.3.1.3 TA(trusted Authority)

TA시스템은 DCAS 시스템에서 3rd Party 구성요소로 설계되었으며, DCAS HOST를 위한 SM, TP의 인증서를 발행하고, LKS의 인증정보 요청 시 인증정보를 전달하는 역할을 수행한다.

IV. 모바일 IPTV에서의 DCAS 보안 문제점 분석 및 안전한 프레임워크 제안

본 장에서는 기존 OpenCable 기반의 DCAS 시스템을 모바일 IPTV 기반의 DCAS 시스템으로 전환 시 발생 가능한 보안 문제점에 대해서 점검하고 이를 해결하기 위해 필요한 보안 프레임워크를 제안한다. 그러한 보안 프레임워크를 운용하기 위해 필요한 보안 요구사항을 도출하고, 이러한 보안 요구사항을 만족시킬 수 있는 모바일 IPTV에서의 안전한 DCAS 보안 프레임워크를 제안한다.

4.1 보안 문제점 분석

4.1.1 DCAS 서버와 DCAS 호스트 간 공유키 관리

DCAS 서버와 DCAS 호스트 간의 상호인증을 위해서 PSK(Pre-Shared Key)는 반드시 안전한 방법으로 각 객체에 분배되어야 한다. 하지만, PSK가 어떻게 분배되는지에 대해서는 OpenCable 규격에서는 정의하고 있지 않다. 또한 방송 콘텐츠를 디스크램블링 하는데 있어서 마스터 키 역할을 하는 DK(Distribution Key) 또한 안전하게 DCAS 서버와 DCAS 호스트에게 분배되어야 한다. 하지만, 기존의 DCAS가 스마트카드 등으로 DK를 DCAS 호스트에게 전달할 수 있는 반면에 모바일 환경에서는 스마트카드를 읽을 수 있는 별도의 장치를 구비하는 것이 어렵기 때문에 스마트카드를 이용한 전달방법은 용이하지가 않다. 따라서 DCAS 서버와 DCAS 호스트 간의 상호인증을 위해서 PSK나 DK가 DCAS 호스트에게 안전하게 전달하기 위한 새로운 보안 메커니즘이 필요하다.

4.1.2 DCAS 서버와 DCAS 호스트의 상호 인증

현재 OpenCable의 DCAS 규격에서는 DCAS 서버와 DCAS 호스트가 공유키를 이용해 상호인증을 수행하도록 정의하고 있지만, 구체적인 인증 메커니즘에 대해서는 별도로 정의하고 있지 않다. 특히 DCAS 클라이언트의 다운로드는 DCAS PS를 이용하게 되는데, DCAS PS와 DCAS 호스트 간의 인증 방법에 대해서는 언급하고 있지 않다. 이 경우, DCAS PS로 위장하여 DCAS 호스트에게 적법한 DCAS 클라이언트인 것처럼 위장하여 다운로드 시킨 후, DCAS 호스트를 감염시킬 수 있다. 즉, 공격자는 DCAS PS가 DCAS 호스트로 적법한 DCAS 클라이언트를 다운로드하는 행위를 차단하고, DCAS PS로 위장하여 변조된 클라이언트 프로그램을 DCAS 호스트에게 다운로드하게 할 수 있다.

이러한 공격은 DCAS AP와 DCAS 호스트 간의 인증이 완료된 이후에 이루어지기 때문에 위험성이 더욱 크다고 할 수 있다. 한편, DCAS AP와 DCAS 호스트 간의 상호인증 역시 구체적인 인증 메커니즘이 정의되어 있지 않기 때문에 구현에 따라서 인증 메커니즘으로 인한 보안 취약성이 발생할 수 있다.

4.1.3 DCAS 클라이언트 보호

OpenCable의 DCAS 규격에서는 DCAS 서버로부터 다운로드 되는 DCAS 클라이언트의 보호 방안에 대해서는 별도로 기술하고 있지 않기 때문에, 이는 OpenCable의 'Common Download' 규격을 참조할 필요가 있다. 'Common Download' 규격에서는 다운로드 되는 소프트웨어에 단말 제조업체가 전자서명을 첨부하도록 하여 다운로드 되는 소프트웨어의 신뢰성을 보장하도록 하고 있다. 그러나 'Common Download' 규격에서는 전자서명을 통한 소프트웨어의 신뢰성 이외에 콘텐트의 기밀성을 보장하지 않는다. 이는 DCAS 호스트가 다운로드 하는 소프트웨어에 대한 정보가 공격자에게 유출될 경우 역공학 등의 방법을 이용해서 공격자가 소프트웨어를 변조할 가능성이 있다. 일반적으로 셋톱박스에 침입하여 소프트웨어를 변조하는 것보다는 네트워크상에서 소프트웨어의 내용을 도청하여 이를 변조하는 것이 더 용이하다. 이와 같은 네트워크상의 DCAS 클라이언트의 보호의 문제는 DCAS PS와 DCAS 호스트 사이에서 DCAS 클라이언트 암호화를 위한 키 분배 메커니즘

이 존재하지 않기 때문에 발생한다.

4.1.4 DCAS 서버 구성요소 간 보호

OpenCable 규격에서는 DCAS 서버를 구성하고 있는 하위 서버들(DCAS LKS, DCAS AP, DPS, DCAS PS) 간의 보안 서비스에 대해서는 별도로 정의하고 있지 않기 때문에, 하위 서버들 간 아래와 같은 보안 문제가 발생할 수 있다.

(1) 비밀 정보 유출: LKS에는 DCAS AP가 사용하는 모든 키가 저장되어 있다. 따라서 이 두 하위 서버간 보안 메커니즘이 존재하지 않는 다면 관련 키 정보가 공격자에게 노출될 수 있다.

(2) 다운로드 정책 유출: 다운로드 프로파일, 다운로드 일정 등 다운로드 정책 정보는 DPS로부터 DCAS AP로 전송된다. 만일 이러한 다운로드 정책 정보가 공격자에게 노출된다면, 공격자는 다운로드 되는 소프트웨어를 더욱 유연하게 접근할 수 있는 기회가 주어진다.

(3) 하위 서버 위장 공격: 공격자는 하위 서버들 간 통신 도청에서 취득한 정보를 바탕으로 DCAS AP, DCAS LKS, DPS, DCAS PS 등으로 위장할 수 있다. 예를 들어 LKS로 위장함으로써 DCAS AP가 DCAS 호스트와의 상호인증을 방해하거나, DCAS AP로 위장함으로써 다운로드 정책을 유출할 수 있다.

4.2 모바일 IPTV에서의 DCAS 보안 요구사항

DCAS 시스템의 보안 요구사항에 대해 [13]에서 "OpenCable DCAS Specification, Host Device 2.5 Core Functional Requirements"에 근거하여 기본적인 보안 요구사항과 추가적인 보안요구사항에 대해 분석해 놓았다. 본 절에서는 [13]에서 분석한 보안 요구사항들에 대해 우선적으로 간략히 살펴보고자 한다.

- 보안 요구사항 1: 호스트는 DOCSIS, OpenCable, OCAP 규격에 따라 플랫폼 코드를 다운로드 할 때, 무결성과 전자서명을 검증해야 한다.
- 보안 요구사항 2: 유효하지 않은 플랫폼 코드로 판단될 경우에는 정해진 규칙에 따라 에러 처리해야 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 상호 인증을 수행해야 한다.
- 보안 요구사항 8: DCAS AP와 DCAS LKS는 상호 인증을 수행해야 한다.
- 보안 요구사항 9: DCAS AP와 DPS는 상호인증을 수행해야 한다.
- 보안 요구사항 10: DCAS AP와 DCAS PS는 상호 인증을 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 LKS 간의 통신 내용은 기밀성과 무결성이 보장되어야 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, 부인봉쇄 가 가능해야 한다.
- 보안 요구사항 17: DCAS PS와 DCAS 호스트 간의 통신 내용은 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 요구사항들이며, 보안 요구사항 6~17까지는 [13]에서 DCAS의 네트워크 보안을 위하여 추가적으로 제기한 보안 요구사항들이다.

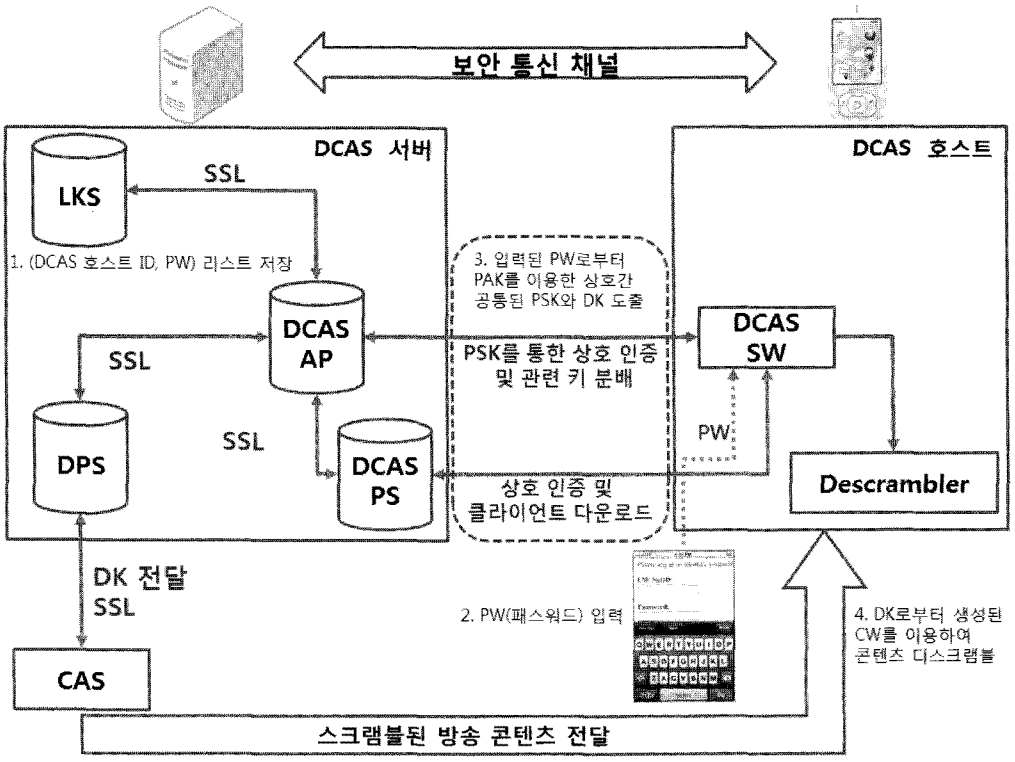
일반적인 DCAS 시스템에서는 DCAS 호스트가

DCAS 클라이언트를 다운로드하기 위해 DCAS AP와 DCAS 호스트 간의 상호인증에 사용되는 PSK를 미리 공유할 필요가 존재하며, 스크램블된 방송 콘텐츠를 DCAS 호스트가 디스크램블하기 위해 요구되는 마스터 키 역할을 하는 DK를 스마트카드와 같은 저장 매체를 통하여 DPS와 DCAS 호스트 간에 공유한다. 그러나 이러한 DCAS 서버와 DCAS 호스트 간 PSK와 DK에 대한 비밀 정보 공유는 기존의 정적인 네트워크에서 휴대가능한 모바일 기기를 이용하는 네트워크로 전환되면서 추가적인 보안 요구사항을 야기한다. 그 이유는 스마트 폰과 같은 모바일 기기에서 스마트 카드와 같은 저장 매체를 읽을 수 있는 장치를 추가적으로 고려하기란 어려운 일이며, 또한 PSK와 같은 비밀 정보 공유를 위해 스마트 폰 메모리상에 그대로 PSK를 저장하는 것은 분실의 위험이 큰 모바일 기기 특성 상 바람직하지 않기 때문이다. 특히 기존 DCAS 시스템에 비하여 분실 및 도난의 위험이 따르는 모바일 기기의 특성을 고려하였을 때, 비밀정보를 모바일 기기의 메모리에 저장하는 것은 바람직하지 않다. 비록 PSK나 DK와 같은 비밀 정보를 암호화하여 모바일 기기에 저장한다 할지라도, 공격자가 사전 조사 혹은 전수 조사 공격 등으로 비밀 정보를 획득할 수 있기 때문이다. 따라서 모바일 IPTV에서의 DCAS 사용을 위해서는 아래와 같은 보안 요구사항들이 추가적으로 요구된다.

- 보안 요구사항 18: DCAS AP와 DCAS 호스트 간 PSK는 안전한 방법으로 공유되어야 한다.
- 보안 요구사항 19: DPS와 DCAS 호스트 간 DK는 안전한 방법으로 공유되어야 한다.
- 보안 요구사항 20: PSK와 DK 정보는 어떤 식으로든지 모바일 기기에 저장되어서는 안된다.

4.3 모바일 IPTV에서의 안전한 DCAS 보안 프레임워크 제안

본 절에서는 앞 절에서 제기한 보안 요구사항들을 만족시키는 모바일 IPTV에서의 안전한 DCAS 보안 프레임워크에 대해서 논의 한다. 기존 OpenCable의 DCAS 시스템 구조를 변경하지 않으면서 동시에 모바일 기기가 CAS 클라이언트를 안전하게 다운로드하고, 방송 콘텐츠를 다운로드하게 하기 위해서 본 논문에서 제안한 DCAS 보안 프레임워크는 [그림 2]와 같다.



[그림 2] 모바일 IPTV를 위한 DCAS 보안 프레임워크

[그림 2]는 모바일 IPTV를 위하여 본 논문에서 제안한 DCAS 보안 프레임워크를 나타내며, 특히 전 절에서 나열한 보안 요구사항 중 보안 요구사항 18~20를 만족시키기 위한 절차를 보여주고 있다. 그 절차는 아래와 같이 진행된다.

(1) DCAS 서버는 DCAS 호스트에 대한 DCAS 호스트 사용자 ID(아이디)와 PW(패스워드)를 LKS에 저장하고 있다. LKS는 DCAS AP가 DCAS 호스트 및 DCAS 서버의 다른 구성요소들과 통신하는데 요구되는 모든 키 정보를 저장하고 있기 때문에, 이러한 DCAS 호스트 사용자 ID와 PW를 저장하는데 적합하다고 판단된다.

(2) DCAS 호스트 사용자는 자신이 타당한 사용자임을 검증하기 위하여 스마트폰의 키보드를 이용하여 PW를 입력한다.

(3) 입력된 PW에 기반하여 DCAS 서버와 DCAS 호스트 간에 PAK(Password-authenticated key exchange protocol, 패스워드 기반 키 교환 프로토콜)를 수행하여 두 객체 간 공통된 PSK와 DK를 도출한다.

(4) 도출된 DK로부터 생성된 CW를 이용하여 콘텐츠 사업자가 CAS를 통하여 제공하는 스크램블된 방송 콘텐츠를 DCAS 호스트에서 디스크램블 한다.

위 절차에서 보듯이 PAK를 이용하여 DCAS 서버와 DCAS 호스트 간 PW 기반의 PSK, DK 공유를 수행할 수 있다. 기존에 다양한 PAK가 제안되었지만, 본 논문에서는 그 중 2007년에 제정된 ITU-T 표준인 X.1035 를 사용한다[14]. ITU-T 에서 권장하는 PAK는 [그림 3]과 같다.

[그림 3]에서의 P는 $A|B|PW$로 이루어지며, 이때 A는 DCAS 호스트 ID이며 B는 DCAS 서버의 ID에 해당한다. 위와 같은 PAK 프로토콜을 통하여 최종적으로 생성되는 K를 이용하여 다양한 방법으로 PSK와 DK를 도출할 수 있다. 예를 들어 PSK= H(K,1), DK=H(K,2)와 같이 일방향성 해시 함수(H(·,·))를 이용하여 하나의 도출된 비밀 정보를 바탕으로 다수의 비밀 정보를 안전하게 생성할 수 있다.

4.4 제안 모델 적용으로 인한 개선 사항 평가

Party A		Party B
$X = H_1(P) \cdot (g^{R_A} \bmod p)$	$\xrightarrow{X}$	Verify that received value is not 0 $\frac{H_1(P) \cdot (g^{R_A} \bmod p)}{H_1(P)} = g^{R_A} \bmod p$
$S_1 = H_3(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$ Calculate S_1 and verify that it is equal to the received value for S_1 from B	$\xleftarrow{S_1, Y}$	$S_1 = H_3(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$ $Y = H_2(P) \cdot (g^{R_B} \bmod p)$
$S_2 = H_4(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$	$\xrightarrow{S_2}$	$S_2 = H_4(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$ Calculate S_2 and verify that it is equal to the received value for S_2 from A
$K = H_5(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$		$K = H_5(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$

[그림 3] ITU-T X.1035에서의 PAK 프로토콜 상세

본 장에서는 본 논문에서 제안한 DCAS 보안 프레임워크를 모바일 IPTV 환경에 적용하였을 때, 개선되어지는 사항들에 대해서 논의한다. 우선 보안 요구사항 1~17에 해당하는 부분은 이미 [13]에서 다루었기 때문에 별도로 다루지 않으며, 모바일 IPTV 환경에서 추가적으로 고려되어지는 보안 요구사항 18~20에 대해서 다룬다.

- 보안 요구사항 18~19: 본 논문에서 제안한 모바일 IPTV에서의 DCAS 보안 프레임워크에서는 ITU-T X.1035에서 권장하는 PAK 프로토콜을 적용하여 DCAS AP와 DCAS 호스트, DPS와 DCAS 호스트 간 각각 PSK와 DK를 생성한다. 기존 OpenCable 방식과 비교하자면, 기존 OpenCable 방식의 DCAS에서는 PSK와 DK와 같은 키 정보를 사전에 미리 스마트카드와 같은 다양한 물리적 수단 등으로 DCAS 호스트와 DCAS 서버가 공유하는 반면에, 본 논문에서 제안한 모바일 IPTV에서의 DCAS 보안 프레임워크에서는 필요시 DCAS 호스트 사용자가 패스워드를 입력하여 안전하게 DCAS 서버와 PSK와 DK를 공유한다. 이에 더하여 기존 DCAS 에서는 PSK와 DK 노출 시, 스마트카드 재발급 등 추가적인 비용이 요구되나, 본 논문에서 제안한 DCAS 보안 프레임워크에서는 PAK를 사용함으로써, 단순히 패스워드 변경이나, 타임스탬프 또는 난수값 변경 등으로 쉽게 갱신이 가능하다.
- 보안 요구사항 20: PSK와 DK 정보는 어떤 형태로든지 모바일 기기에 저장되어서는 안 된다. 본 논문에서 제안한 모바일 IPTV에서의 DCAS 보안 프레임워크에서는 PSK와 DK를 얻어낼 수

있는 데이터를 별도로 모바일 기기 내에 저장하지 않는다. 그 이유는 제안한 DCAS 보안 프레임워크에서는 PAK 프로토콜을 하에서 DCAS 호스트 사용자가 타당한 패스워드를 입력함으로써 DCAS 서버와 연동하여 상호 인증 후, PSK와 DK가 설립되기 때문이다.

V. 결 론

최근 스마트폰 시장의 급성장은 향후 모바일 IPTV의 활성화에 더욱 박차를 가하는 계기가 될 것이며 이는 미래의 정보통신산업에 큰 영향을 미칠 것으로 예상 된다. 새롭게 시작되는 모바일 IPTV 서비스 산업 발전을 위해서는 모바일 IPTV 콘텐츠 저작권 보호를 위한 조치들이 마련되어야 한다.

기술적 보호 조치는 디지털 콘텐츠의 불법복제방지 및 저작권보호를 위해 가장 중요한 요소이며, 소프트웨어 기반의 제한수신 시스템 DCAS는 디지털 콘텐츠 유통에 있어 가장 널리 사용되는 중요한 기술이다. 또한 모바일 IPTV 환경에서 DCAS 시스템은 콘텐츠 보호기술간 상호 호환성, 침해 시 빠른 대처, DRM등 다른 서비스와의 연동이 효율적으로 이루어지는 여러 장점을 갖고 있어 많은 활성화가 기대된다.

하지만 모바일 IPTV에 DCAS 시스템이 적용되기 위해서는 발생 가능한 보안 문제점에 대해서 점검하고 보안 모델을 수립하고 분석해 볼 필요가 있다. 본 논문에서는 이러한 필요성에 의해 모바일 IPTV환경에서의 안전한 DCAS 보안 프레임워크 제시하였고, 이를 기반으로 하여 모바일 IPTV 환경에서 추가적으로 고려되어야 하는 보안 요구사항을 도출하였다.

본 연구는 결과는 현재 국내외적으로 진행 중인 모바일 IPTV 서비스 보안 시스템의 안전성 및 신뢰성을 확보할 수 있는 보안 기술을 제공하며 모바일 IPTV 국제 표준화 기관에서 표준화를 선도하는데 활용될 수 있다.

참고문헌

[1] http://en.wikipedia.org/wiki/Mobile_IPTV

[2] Carlsson. C and Walden. P, "Mobile TV - To Live or Die by Content," IEEE 40th Annual Hawaii International Conference on System Sciences, pp. 51-60, Jan. 2007.

[3] Djama. I and Ahmed. T, "A Cross-Layer Interworking of DVB-T and WLAN for Mobile IPTV Service Delivery," IEEE Transactions on Broadcasting, Vol. 53, No. 1, pp. 382-390, Feb. 2007.

[4] Retnasothie. Francis E, "Wireless IPTV over WiMAX", Challenges and Applications, Wireless and Microwave Technology Conference 2006, WAMICON 06, pp. 1-5, 2006.

[5] Hartung. F, "Delivery of Broadcast Service in 3G Networks," IEEE Transactions on Broadcasting, Vol. 53, No. 1, pp. 188-196, Mar. 2007.

[6] 박수홍, "Mobile IPTV 기술 및 국내외 표준화 동향," TTA Journal, No.114, pp. 50-52, Nov 2007.

[7] A. M. Eskicioglu, "Protecting Intellectual Proprety in Digital Multimedia Networks," IEEE Computer, Vol. 36, pp. 39-45, Jul. 2003.

[8] H. Benoit, "Digital Television-MPEG-1, MPEG-2 and principles of the DVB System," Focal Press, S데. 2002.

[9] B. Rosenblatt, B. Trippe, and S. Mooney, "Digital Rights Management," Business and Technology, M&T Books, Dec. 2001.

[10] 한국소프트웨어진흥원, "DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구," 2004년 2월.

[11] 김민영, "DCAS를 위한 보안 메커니즘," 석사학위논문, 충남대학교, 2009년 2월.

[12] 김영모, 고병수, "다운로드형 제한수신시스템 기술동향," 한국방송공학회지, 제13권 제 4호, pp. 54-64, 2008년 12월.

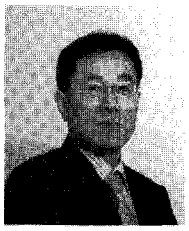
[13] 강성구, "안전한 다운로드 가능 제한 수신 시스템 제안 및 구현," 한국정보보호학회지, 제19권 제 6호, pp. 165-166, 2009년 12월.

[14] ITUT2007 "SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY: Password-authenticated key exchange (PAK) protocol", ITU-T, X.1035, 2007.

〈著者紹介〉

최 중 영 (Jung-Young Choi) 정회원
2005년 2월: 중앙대학교 산업정보학과 졸업
2008년 9월~현재: 고려대학교 정보경영공학전문대학원 석사과정
〈관심분야〉 포렌식어카운팅, 디지털포렌식, 정보보호정책, 개인정보보호, 저작권 등

조 관 태 (Kwantae Cho) 정회원
2005년 2월: 고려대학교 컴퓨터학과 졸업
2008년 2월: 고려대학교 정보경영공학전문대학원 석사
2008년 3월~현재: 고려대학교 정보경영공학전문대학원 박사과정
〈관심분야〉 키 교환, USN 보안, IPTV 보안, VANET 보안



임 종 인 (Jong-in Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
現 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장 (고려대학교 정보보호연구원 원장 겸임), 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 한국저작권위원회 위원 등
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등