情報保護學會論文誌
第19卷 第6號, 2009. 12

안전한 다운로드 가능 제한 수신 시스템 제안 및 구현*

강 성 구,[1†] 박 종 열,[2] 백 의 현,[2] 박 춘 식,[3] 류 재 철[1‡]
[1]충남대학교, [2]한국전자통신연구원, [3]서울여자대학교

Technique and Implementation of Secure Downloadable Conditional Access System*

Seong-Ku Kang,[1†] Jong-Youl Park,[2] Eui-Hyun Paik,[2] Choon-Sik Park,[3]
Jae-Cheol Ryou[1‡]
[1]Chung-Nam National University,
[2]Electronics and Telecommunications Research Institute, [3]Seoul Woman University

요 약

IPTV에서는 제한수신시스템(Conditional Access System, CAS)을 사용하여 자격을 갖춘 시청자 만이 시청이 가능하도록 한다. 현재까지 CAS는 set-top box 혹은 cable card를 이용하여 사용자에게 서비스를 제공하는 것이 일반적이었지만 근래에는 기기간 호환성 문제 해결, DRM 등 다른 서비스와의 연동 문제 해결, 안전성 확보 등을 이유로 다운로드 가능한 CAS 시스템(Downloadable CAS, DCAS)에 대한 연구가 이루어 지고 있다. 본 논문에서는 오픈 케이블 기반의 DCAS 시스템의 취약성을 분석 및 보완하여 안전한 DCAS 시스템을 제안한다. 또한 제안한 시스템의 구현결과를 보여 요구사항에 대한 만족도를 분석한다.

ABSTRACT

IPTV provides their services only for their subscribers who have a eligibility to watch it by using Conditional Access System(CAS). CAS has been servicing their contents for subscribers by using set-top box or cable card so far, but these days, to solve the compatibility between kinds of devices, linkage with other services as DRM and confirming stability , the research of Downloadable CAS(DCAS) is being advanced steadily. On this paper, we analyse the vulnerability of DCAS based on the OpenCable and make up for the vulnerability in DCAS, then proposes to use secure DCAS system for IPTV. Also we show the result of the research and analyse the satisfaction of requirements.

Keywords: IPTV Security, CAS, DCAS, Network Security

I. 서 론

IPTV는 인터넷을 기반으로 하는 TV 서비스라는 기본 개념을 가지고 있으며, “Internet Protocol TV”, “Interactive Personal TV”, “Intelligent Program TV”라는 3가지 특징을 갖는다. 즉, IP를 기반으로 양방향 서비스가 가능하고 point-to-point 전달방식으로 개인화 된 채널을 시청할 수 있으며, 초고속 인터넷 기반의 VoIP(Voice over IP)서비스와의 결합을 통한 서비스 제공 등이 가능하다. IPTV에서 찾아 볼 수 있는 가장 큰 특징은 방송용 전파가 아닌 인터넷 프로토콜을 이용한 패킷 방식으로 멀티미디어 콘텐츠를 제공한다는 점과 PC가 아닌 TV 단말기를 통해 다양한 서비스를 제공한다는 점이다[1].

이와 같은 IPTV 혹은 디지털 방송은 방송 콘텐츠

접수일(2009년 5월 6일), 게재확정일(2009년 10월 1일)
* 본 연구자는 2009학년도 서울여자대학교 교내학술연구비의 지원을 받았음.
† 주저자, ssabro@cnu.ac.kr
‡ 교신저자, jcryou@cnu.ac.kr

를 보호하기 위한 암호화 기술과 시청자가 일정한 금액을 지불해야만 시청이 가능하게 하는 제한 수신 기술이 필요하다. 즉 CAS는 방송 시스템에 가입자의 개념을 도입하여 수신자격이 있는 시청자만이 보호된 방송 콘텐츠를 시청할 수 있게 하는 시스템이다. 이와 같은 CAS의 클라이언트는 현재까지는 하드웨어로 제작되는 것이 일반적이었으나 최근에는 제한수신 클라이언트를 소프트웨어로 구현하려는 연구 및 개발이 증가하고 있다. 이는 하드웨어적으로 제한수신 클라이언트를 구현하는 경우에 발생할 수 있는 다음과 같은 문제점들을 해결하기 위해서이다.

호환성 부족: 하드웨어로 구현된 CAS 클라이언트의 경우에는 하나의 서비스 제공자에 맞추어 출시되므로 동시에 여러 서비스 제공자로부터 서비스를 받기가 어렵다.

다른 서비스와의 연동: 최근 지적재산권의 중요성이 강조되면서 DRM (Digital Right Management) 등에 대한 관심이 높아지고 있는 가운데, 하드웨어로 구현된 CAS는 기존 클라이언트에 새로운 서비스를 추가하기가 어렵다.

안전성: 하드웨어로 구현된 제한수신 시스템이 키 정보의 보호 등에 있어서 안전성이 높은 것은 사실이나, 제한수신 시스템에 내장된 암호 알고리즘이 크랙(Crack)되거나 키 정보가 누출된 경우에는 이의 대체가 쉽지 않다. 즉, 하드웨어의 교체 이외에는 보안 사고에 대처할 방법이 없다.

한 편, 미국 연방통신위원회(FCC: Federal Communication Commission)는 셋톱박스에서 보안 기능을 분리하도록 의무화하고 있다. 이와 같은 내용을 실현하기 위해서 셋톱박스 개발업체는 케이블카드의 교체가 가능하도록 하는 방식으로 구현하는 것이 일반적이었으나 최근에는 소프트웨어 다운로드 방식의 DCAS가 포함되는 추세이다.

DCAS는 S/W 다운로드 방식을 취하여 여러 가지 장점을 얻는다. 서비스 간 혹은 서비스 제공자 간 유연한 서비스 연동성을 갖으며 기존 시스템의 취약점 발견 시 해당 취약점을 바로 패치하거나 기존 시스템을 업그레이드 하여 큰 비용의 지출 없이 취약점을 보완할 수 있다는 장점이 있다.

하지만 현재 제안되어 있는 DCAS는 여러 가지 문제점을 가지고 있다. 인터넷 기반인 IPTV는 기존에 인터넷이 가지고 있는 다양한 문제점을 상속받는다. 따라서 악성코드의 피해와 이로 인하여 서비스 장애 및 경제적 손실 등이 가능하다. 또한 접근성이 보다 쉬워지면서 공격 가능성이 높아 질 수 있다. 특히 DCAS 서버 및 클라이언트의 위장 공격, 컨텐츠의 도청 등의 공격이 위협 요소로 지적될 수 있다.

따라서 본 논문에서는 OpenCable의 DCAS를 적용하는데 있어서 발생 가능한 보안 취약점을 도출하고 이를 해결할 수 있는 안전한 DCAS 시스템을 제안하여 구현한다. 또한 구현된 결과물에 대하여 분석한 내용과 비교, 분석한다. 본 논문의 2장에서는 기존 CAS와 DCAS의 구조 및 동작 방식에 대하여 살펴보고 3장에서는 OpenCable에서 제안된 DCAS 구조의 보안 문제점을 진단하고 해당 문제점을 보완하여 안전한 DCAS 시스템을 설계 및 제안한다. 4장에서는 3장에서 제안한 내용을 바탕으로 구현된 DCAS 시스템을 분석하고 5장으로 결론을 맺는다.

II. 관련 연구

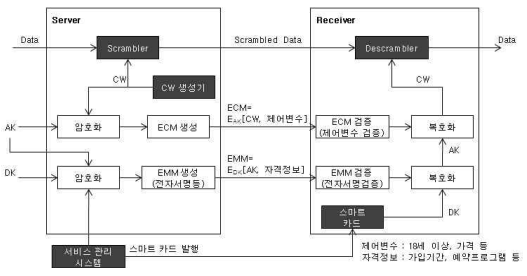
본 장에서는 CAS 및 DCAS의 구조와 기능에 대하여 살펴본다.

2.1 CAS

CAS는 콘텐츠 보호를 위해 방송 시스템에 가입자(Subscriber)의 개념을 도입하여 수신자격(Entitlement)이 있는 시청자만이 서비스를 이용 가능하도록 한 시스템이다. 일반적으로 [그림 1]과 같은 구조를 가지며 제공하는 기능은 다음과 같다.

2.1.1 스크램블링 / 디스크램블링 (Scrambling/Descrambling)

수신자격이 없는 수신자는 시청이 불가능 하도록 데이터를 스크램블링 하는데 이때 방송 콘텐츠는 제어단어(CW : Control Word)를 이용하여 처리된다.



[그림 1] 일반적인 CAS 구조

제어단어는 암호화되어 스크램블링된 방송 데이터와 함께 전송되며 수신자는 암호화된 제어단어를 복호화하고 이를 이용해서 방송 데이터의 디스크램블링을 수행한다.

2.1.2 자격 제어(Entitlement Control)

제어단어를 인증키(AK: Authentication Key)로 암호화하고, 이를 ECM (Entitlement Control Message)에 포함시켜 수신자에게 전송한다. 즉, ECM은 'EAK[CW,제어변수]'와 같은 형태를 지닌다. 제어단어는 주기적으로 전송되며, 그 때마다 제어단어가 새롭게 생성되고 암호화된다. ECM에는 암호화된 제어단어 외에 제어변수가 포함된다. 수신자는 제어단어를 복호화하고, 이를 이용하여 수신된 방송 데이터를 디스크램블링 한다.

2.1.3 자격 관리(Entitlement Management)

수신기에 자격을 부여·갱신·관리하는 기능을 하며, 인증키를 분배키(DK: Distribution Key)로 암호화하여 EMM (Entitlement Management Message)을 생성하고 수신자에게 전송한다. 즉, EMM은 'EDK[AK, 자격정보]'와 같은 형태를 갖게 된다. 따라서 송신자와 수신자는 반드시 같은 비밀키인 분배키(DK)를 공유하여야 하며, 이러한 비밀키를 공유하는 과정에서 보안성을 높이기 위해 스마트 카드 등의 하드웨어를 이용하는 것이 일반적이다.

2.2 OpenCable DCAS

2.2.1 일반적인 DCAS 개요

DCAS는 소프트웨어의 안전한 다운로드를 위해 미국의 케이블 방송 전문연구기기관인 CableLabs에 의해서 제안된 기술이다. 주요 내용은 서비스 보호 기술을 데이터 방송을 위한 미들웨어 표준인 OCAP(OpenCable Applicaation Platform) 호환 사용자 미디어 장치 내에서 사용 가능하도록 하는 제한수신 클라이언트(컴퓨터 프로그램)의 안전한 다운로드에 대해서 다룬다.

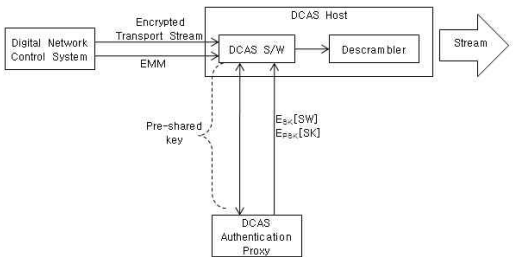
DCAS는 2004년 8월에 제안되었으나, 아직까지 드래프트에 머물고 있다. 이는 초기에는 보안모듈이 분리되어야 한다는 미국 연방통신위원회(FCC: Federal Communications Commission)의 요구사항을 만족시키지 못했고 주요 단말 제조업체의 협력이 매우 부진했기 때문이다. 이에 따라 2006년 2월에 드래프트가 공개되어 현재까지 표준화가 진행 중이다.

케이블카드를 소프트웨어로 대체하게 되는 DCAS의 가장 큰 목적 가운데 하나는 디지털 TV, DVR (Digital Video Recorder), 셋톱박스 등의 OCAP 호환 장치에서 DRM 기술을 소프트웨어적으로 구현하는 것이라고 할 수 있다. 즉, DCAS를 통해서 케이블 방송사와 사용자 장치 사이의 전송 정보를 보호할 수 있으며, '재생 후 즉시 삭제', '재생 기간 설정', '녹화 제한' 등과 같이 콘텐츠의 이용을 관리할 수 있다.

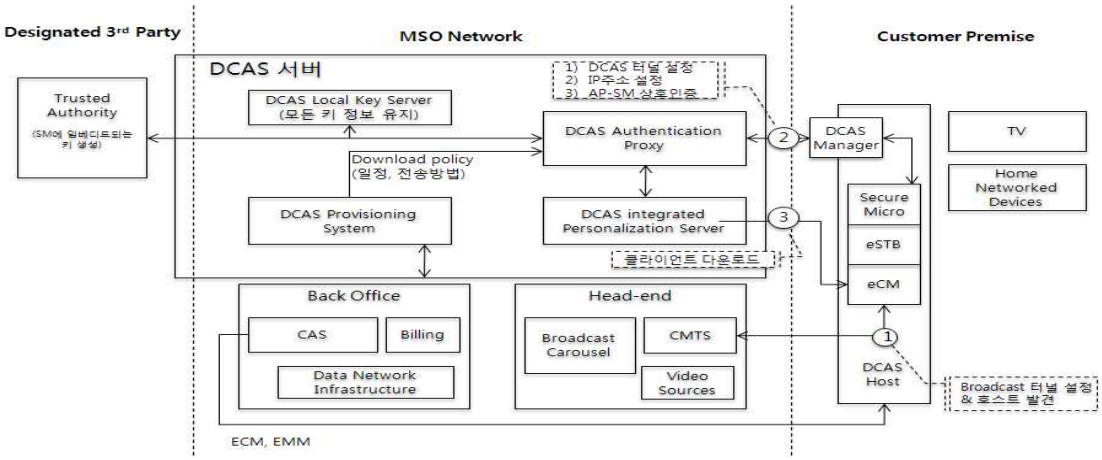
DCAS가 적용될 경우 얻을 수 있는 또 하나의 장점은 안전성의 향상이다. 예를 들어 어떤 암호화 알고리즘이 크랙되는 경우가 발생할 경우, DCAS 기술을 통해서 알고리즘의 대체가 쉽게 이루어질 수 있다. 즉, 기존에는 이와 같은 문제가 발생할 경우에는 하드웨어의 교체가 불가피했지만, DCAS가 적용된다면 소프트웨어의 업데이트만으로 문제의 해결이 가능하게 된다.

[그림 2]는 일반적인 DCAS 시스템을 개념적으로 설명한다. 스크램블된 영상을 디스크램블 할 때는 전송키(transport key)가 사용되며, 전송키의 보호를 위해서는 EMM 키가 사용됨은 이미 앞에서 설명한 일반적인 CAS 구조와 동일하다. DCAS 시스템이 동작하는 과정을 살펴보면 [그림 3]과 같다.

0) DCAS AP(Authentication Proxy)와 DCAS 호스트는 미리 공유된 키(PSK)를 소지하고 있다.
1) CAS 클라이언트 프로그램을 다운로드 해야 할 때, 이를 위해서 DCAS AP는 우선 DCAS 호스트를 발견하기 위한 메시지를 브로드 캐스트 한다.
2) DCAS 호스트가 (1)의 메시지에 응답함으로써 DCAS AP는 셋톱박스를 식별할 수 있다.



[그림 2] DCAS 시스템 개념



[그림 3] CAS 시스템 구조

3) DCAS AP는 다운로드 될 CAS 클라이언트 프로그램을 암호화 하는 데 사용될 암호키를 DCAS 호스트에게 전송한다. 이 때, 암호키를 암호화하기 위해 미리 공유된 키가 사용된다.
4) AP는 3)에서 전달된 암호키로 CAS 클라이언트 프로그램을 암호화하여 DCAS 호스트에게 다운로드 한다. 이후 DCAS 호스트 내에서 CAS 클라이언트가 정상적으로 동작하게 된다.
5) 방송 시스템은 방송 콘텐츠를 스크램블 하는데 사용되는 키(제어단어)를 DCAS 호스트에게 전송한다.
6) 방송 시스템은 스크램블된 방송 콘텐츠를 DCAS 호스트에게 전송한다.

2.2.2 DCAS 시스템 구조

DCAS 시스템은 키 관리, 다운로드 프로토콜, 전송 요구사항 등을 포함하며, 시스템 구조는 그림 3과 같다.

[그림 3]의 DCAS 시스템 구조에서 DCAS가 DCAS 네트워크 서비스를 이용하기 위해 제일 먼저 접근하는 구성요소는 AP이며, AP는 DCAS 호스트에게 DCAS 메시지를 전송하고 DCAS 호스트의 요청에 응답한다. ①은 DCAS 호스트 간의 상호인증을 수행하는데 사용되며 ②는 DCAS 터널로서 발견된 DCAS 호스트의 IP 및 기타 필요한 사항을 설정하고 DCAS AP와 DCAS 호스트 간의 상호인증을 수행하는데 사용된다. 그리고 ③에서 실질적인 DCAS 클라이언트의 다운로드가 이루어진다[2].

III. DCAS 보안 문제점 분석 및 안전한 DCAS 시스템 제안

본 장에서는 OpenCable 기반의 DCAS 시스템에 대한 보안 문제점을 점검하고 요구사항을 도출하고 그 내용을 바탕으로한 안전한 DCAS 시스템을 위해 필요한 보안 서비스를 제안한다. 이를 위해서 우선, DCAS 시스템을 안전하게 운용하기 위해서 필요한 보안 요구사항을 정의하고, 앞서 살펴본 DCAS의 보안상 문제를 해결하기 위해 필요한 보안 서비스를 정의한다.

3.1 보안 문제점 분석

3.1.1 DCAS 서버와 DCAS 호스트의 상호 인증

현재 오픈케이블의 DCAS 규격에서는 DCAS 서버와 DCAS 호스트가 공유키를 이용해 상호인증을 수행하도록 정의하고 있지만, 구체적인 인증 메커니즘에 대해서는 별도로 정의하고 있지 않다. 특히 DCAS 호스트의 다운로드는 DCAS PS를 이용하게 되는데, DCAS PS와 DCAS 호스트 간의 인증 방법에 대해서는 언급하고 있지 않다.

이 경우, DCAS PS로 위장하여 DCAS 호스트에게 안전하지 않은 DCAS 클라이언트를 다운로드 하도록 하는 공격이 가능하다. 즉, 공격자는 DCAS PS가 DCAS 호스트로 S/W를 다운로드 하는 행위를 차단하고, DCAS PS로 위장하여 변조된 클라이언트 S/W를 DCAS 호스트에게 다운로드하게 할 수 있다.

이와 같은 공격은 DCAS AP와 DCAS 호스트 간의 인증이 완료된 이후에 이루어지기 때문에 위험성이 더욱 크다고 할 수 있다.

한 편, DCAS AP와 DCAS 호스트 간의 상호인증 역시 구체적인 인증 메커니즘이 정의되어 있지 않기 때문에 구현에 따라서 인증 메커니즘의 취약성이 발생할 수 있다. 이러한 예는 [3] 등에서 쉽게 찾아볼 수 있다.

3.1.2 DCAS 클라이언트 보호

현재 오픈케이블의 DCAS 규격에서는 DCAS 서버로부터 다운로드 되는 DCAS 클라이언트의 보호 방안에 대해서는 별도로 기술하고 있지 않으며, 이는 오픈케이블의 'Common Download'[4] 규격을 참조해야 한다. [4]에서는 다운로드 되는 소프트웨어에 단말 제조업체가 전자서명을 첨부하도록 하여 다운로드 되는 소프트웨어의 신뢰성을 보장하도록 하고 있다.

그러나 전자서명을 통한 소프트웨어의 신뢰성 검증 이외에 추가적으로 콘텐트의 기밀성을 유지할 필요가 있다. 이는 다운로드 되는 소프트웨어가 공격자에게 유출될 경우에는 역공학 등의 방법을 이용해서 소프트웨어를 변조할 가능성이 커지기 때문이다. 일반적으로 셋톱박스에 침입하여 소프트웨어를 변조하는 것보다는 네트워크상에서 소프트웨어의 내용을 도청하는 것이 좀 더 용이하다.

이와 같은 네트워크상의 DCAS 클라이언트의 보호의 문제는 DCAS PS와 DCAS 호스트 사이에서 DCAS 클라이언트 암호화를 위한 키 분배 메커니즘이 존재하지 않기 때문에 발생한다.

3.1.3 DCAS 서버 구성요소 간 보안

오픈케이블에서는 DCAS 서버를 구성하고 있는 하위 서버들 간의 보안 서비스에 대해서는 별도로 정의하고 있지 않은데, 이럴 경우에는 다음과 같은 문제가 발생할 수 있다.

- 키 정보 유출: DCAS AP가 사용하는 모든 키는 LKS에 보관되도록 되어 있다. 따라서 DCAS AP로부터 LKS로 전송되는 키 정보가 유출될 수 있다.
- 다운로드 정책 유출: 다운로드 일정, 다운로드 방법 등 다운로드 정책 정보는 DPS로부터 DCAS AP로 전송된다. 다운로드 정책 정보가 유출됨으로써 다운로드 되는 S/W에 접근이 용이해질 수 있다.
- 위장 공격: DCAS AP, DCAS LKS, DPS, DCAS PS 등으로 위장할 수 있다. DCAS AP로 위장함으로써 다운로드 정책을 유출하거나, DCAS PS의 가용성을 저해할 수 있다.

3.1.4 키관리

DCAS 서버와 DCAS 호스트의 상호인증에 사용되는 Pre-shared 키가 어떻게 분배되는지에 대해서는 오픈케이블 규격에서 정의하고 있지 않다. 또한 방송 콘텐트를 디스크램블링 하는데 있어서 마스터 키의 역할을 하는 DK는 기존에는 하드웨어 기반의 CAS에서는 스마트카드 등을 이용하여 분배했지만, 하드웨어를 사용하지 않는 DCAS에서는 어떻게 분배 및 관리할 것인지 정의하고 있지 않다.

이와 같이 키 분배 및 관리 방법에 대해서 정의하고 있지 않은 경우에는 구현에 따라서 키가 유출될 위험이 있다. 예를 들어 Pre-shared 키를 온라인 배포한다면 Pre-shared 키 보호를 위한 메커니즘이 또 다시 필요하게 된다.

3.2 안전한 DCAS 시스템 제안

3.2.1 DCAS 보안 요구사항

본 절에서는 DCAS 시스템의 안전성 확보를 위해 필요한 DCAS 보안 요구사항을 도출한다. 우선 [5]에 근거하여 DCAS 호스트의 보안 요구사항을 살펴보면 다음과 같다.

- 요구사항 1: 호스트는 DOCSIS, 오픈케이블, OCAP 규격에 따라 플랫폼 코드를 다운로드 할 때, 무결성과 전자서명을 검증해야 한다.
- 요구사항 2: 유효하지 않은 플랫폼 코드로 판단될 경우에는 정해진 규칙에 따라 에러 처리해야 한다.
- 요구사항 3: 호스트는 전자서명이 첨부되어 있고, 첨부된 전자서명의 유효성이 검증된 플랫폼 코드만을 실행시켜야 한다.
- 요구사항 4: 호스트 플랫폼 코드는 DOCSIS, 오픈케이블, OCAP에 정의된 바에 따라 RSA 전자서명을 첨부하고 있어야 한다.

- 요구사항 5: 호스트는 코드의 실행 중 변경을 허용하지 않는다.

위에서 살펴본 바와 같이 [5]에서 정의하고 있는 보안 요구사항은 DCAS 호스트 시스템에 필요한 것으로 네트워크와 관련된 보안 요구사항은 포함하고 있지 않다. 이에 따라 본 논문에서는 앞서 살펴본 보안 문제점을 해결하고, DCAS 시스템의 안전성 확보를 위한 네트워크 보안 요구사항을 다음과 같이 도출하였다.

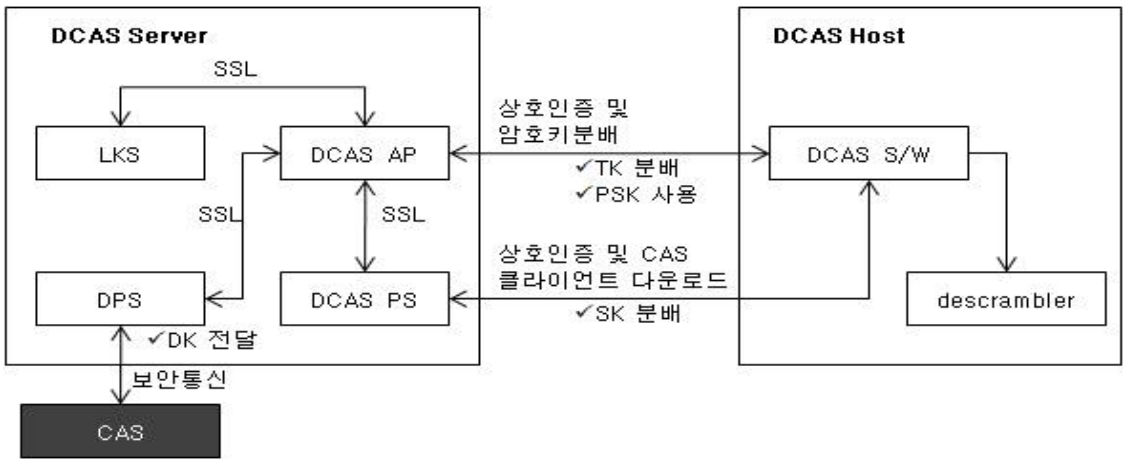
- 요구사항 6: DCAS AP와 DCAS 호스트는 상호인증을 수행해야 한다.
- 요구사항 7: DCAS PS와 DCAS 호스트는 상호인증을 수행해야 한다.
- 요구사항 8: DCAS AP와 DCAS LKS는 상호인증을 수행해야 한다.
- 요구사항 9: DCAS AP와 DPS는 상호인증을 수행해야 한다.
- 요구사항 10: DCAS AP와 DCAS PS는 상호인증을 수행해야 한다.
- 요구사항 11: DCAS LKS에게 DCAS AP와 TA와의 통신 이외에 다른 통신은 허용되지 않는다.
- 요구사항 12: DPS는 DCAS AP와의 통신만 허용된다.
- 요구사항 13: DCAS PS는 DCAS AP와의 통신만 허용된다.
- 요구사항 14: DCAS AP와 DCAS LKS 간의 통신 내용은 기밀성과 무결성이 보장되어야 한다.
- 요구사항 15: DCAS AP와 DPS와의 통신 내용은 기밀성과 무결성이 보장되어야 한다.
- 요구사항 16: DCAS AP와 DCAS PS 간의 통신 내용은 기밀성과 무결성이 보장되어야 하며, 부인봉쇄가 가능해야 한다.
- 요구사항 17: DCAS PS와 DCAS 호스트 간의 통신 내용은 기밀성과 무결성이 보장되어야 하며, 부인봉쇄가 가능해야 한다.

요구사항 6과 요구사항 7은 DCAS 서버와 DCAS 호스트의 상호인증에 대해서 다루는 것으로 DCAS AP와 DCAS PS가 논리적으로는 DCAS 서버에 속하는 구성요소라 하더라도, 각각 DCAS 호스트와 상호인증이 필요함을 설명한다. 요구사항 8 ~ 요구사항 10은 DCAS 서버를 구성하고 있는 구성요소 간에 상호인증이 필요함을 설명한다. 요구사항 11 ~ 요구사항 13은 DCAS 서버의 접근제어와 관련된 사항이다. 그리고 요구사항 14 ~ 요구사항 17은 DCAS 구성요소간, DCAS 서버와 DCAS 호스트간 통신보안을 다룬다. 특히 요구사항 16의 경우에는 DCAS AP의 통지에 의해서 DCAS PS가 다운로드 동작을 시작하기 때문에 부인봉쇄가 필요하며, 요구사항 17에서는 다운로드 되는 DCAS 클라이언트 프로그램의 신뢰성 확보를 위해 부인봉쇄가 필요하다.

3.2.2 안전한 DCAS 시스템 구조

안전한 DCAS 시스템은 [그림 4]와 같이 기존 오픈케이블의 DCAS 시스템 구조를 변경하지 않으면서 CAS 클라이언트의 안전한 다운로드 및 방송 콘텐트 시청이 가능하도록 하였다.

[그림 4]에서 DCAS AP는 DCAS 호스트와의 미리 공유된 키(PSK: Pre-Shared Key)를 이용해서



[그림 4] 안전한 DCAS 시스템 구조

상호인증을 수행하고, DCAS 클라이언트를 다운로드 하는데 사용되는 암호키를 DCAS 호스트와 공유하는 역할을 한다. 한 편 DCAS AP가 DCAS 호스트 및 DCAS 서버의 다른 구성요소와 통신하는데 사용하는 모든 키 정보는 LKS에 기록된다.

DCAS PS는 새로운 DCAS 클라이언트 프로그램을 DCAS 호스트에게 다운로드한다. 이 때, DCAS PS는 DCAS AP가 DCAS 호스트와 통신을 위해서 사용했던 채널과는 다른 채널을 사용해서 DCAS 클라이언트 프로그램을 다운로드 하기 때문에 역시 DCAS 호스트와 상호인증을 수행할 필요가 있으며, DCAS AP로부터 암호키를 전달 받아 다운로드 되는 DCAS 클라이언트 프로그램을 암호화 한다.

DPS는 다운로드와 관련된 정책 정보를 생성하여 DCAS AP에게 전달한다. 또한 DCAS AP에 의해서 DK가 갱신되는 경우에는 갱신된 DK를 방송 송신자에게 전달한다.

마지막으로 LKS는 위에서 설명한 바와 같이 DCAS AP가 사용하는 모든 키 정보를 보관한다. 이는 장애, 재난 등으로 인해 DCAS AP가 키 정보를 분실할 경우를 대비하기 위해서이다.

(1) 제안한 DCAS 시스템의 동작 과정은 다음과 같다.

(2) DCAS AP와 DCAS 호스트는 상호인증에 사용되는 PSK를 미리 공유하고 있다.

(3) DCAS AP 혹은 DCAS 호스트에 의해서 새로운 DCAS 클라이언트 프로그램의 다운로드를 요청한다.

(4) DCAS AP와 DCAS 호스트는 PSK를 이용해서 상호인증을 수행한다.

(5) 상호인증이 완료된 후에 DCAS AP는 DCAS PS에게 다운로드 받아야 할 DCAS 호스트의 정보를 전달한다. 이 때, DCAS PS가 DCAS 호스트와 키를 공유하는데 사용될 값을 함께 전달한다.

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

(7) DCAS PS는 DCAS 클라이언트를 암호화하여 DCAS 호스트에게 다운로드 한다. 다운로드가 완료되면 DCAS PS는 DCAS AP에게 다운로드가 완료되었음을 알린다.

(8) DCAS PS로부터 다운로드가 완료되었음을 통보 받은 DCAS AP는 분배키를 DPS에게 전달하여 방송 콘텐트를 암호화하는데 사용하도록 한다.

(9) DCAS 호스트는 DCAS AP 및 DCAS PS와 상호인증 과정에서 공유된 값으로부터 새로운 DK를 생성한다.

(10) DPS는 DCAS AP로부터 전달 받은 DK를 생성하는데 사용되는 값을 CAS 서버에게 전달한다.

CAS 서버는 DK를 이용해서 EMM과 ECM를 DCAS 호스트에게 전달한다.

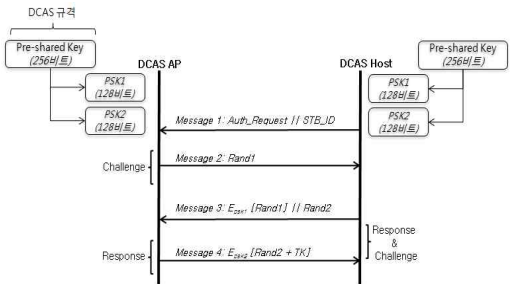
위의 동작과정은 기본적으로 오픈케이블의 DCAS 규격을 따르는 것이다. 그러나 DCAS AP와 DCAS 호스트 간의 상호인증, DCAS PS와 DCAS 호스트 간의 상호인증 절차는 본 논문에서 새롭게 정의하였다. 또한 EMM 암호화에 사용될 CAS의 DK를 생성하고 분배하는 과정과 DCAS 클라이언트 프로그램 암호화에 사용되는 암호 키를 분배하는 과정 역시 본 논문에서 추가한 부분이다.

3.3 개체 간 보안 통신 프로토콜 제안

3.3.1 DCAS AP - DCAS 호스트 상호 인증

(1) DCAS AP와 DCAS 호스트의 상호인증은 처음 DCAS 호스트 설치시 DCAS AP와 DCAS 호스트가 공유하고 있는 키(PSK)가 있다는 가정을 전제한다. DCAS AP와 DCASP 호스트의 상호인증은 Challenge-Response 방식을 따르며, 구체적인 내용은 [그림 5]와 같다.

(2) DCAS AP와 DCAS 호스트는 미리 공유하고 있는 PSK를 2개로 분리하여 psk1과 psk2를 생성한다. PSK를 분리하여 사용하는 이유는 DCAS AP가 Response를 생성할 때 사용하는 키와 DCAS 호스트가 Response를 생성할 때 사용하는 키를 서로 다르게 함으로써 암호 알고리즘으로 스트림 사이퍼를 사



[그림 5] DCAS AP - DCAS Host 상호인증

용할 때 발생할 수 있는 문제를 방지하기 위해서이다.

(3) DCAS AP는 DCAS 호스트에게 Challenge 값 Rand1을 전송한다(Message 2).

(4) DCAS 호스트는 Epsk1[Rand1]과 같이 Response 값을 생성한다. Response 값과 함께 DCAS AP 인증을 위해서 Challenge 값 Rand 2를 전송한다.

(5) DCASP AP는 Epsk1[Rand1]를 계산하여 DCAS 호스트가 전송한 값과 일치하는지 여부를 확인함으로써 DCAS 호스트를 인증한다. 그리고 DCAS 호스트가 전송한 Challenge 값에 대하여 Epsk2[Rand2+TK]와 같이 Response 값을 생성하여 DCAS 호스트에게 전송한다. 이 때, TK는 DCAS PS에게 전달될 임시키이다.

DCAS 호스트는 Epsk2[Rand2+TK]를 복호화하여 그 결과에 자신이 전송한 Rand2가 포함되어 있으면, 정당한 DCAS AP로 간주하고 인증을 완료하며 TK를 저장한다.

3.3.2 DCAS AP - DCAS 호스트 통신

DCAS AP와 DCAS 호스트의 상호 인증 후 호스트의 클라이언트 버전 확인을 위한 통신이 이루어진다. 이때 모든 내용은 TK에 의하여 암호화 된다. 호스트는 AP 측으로 설치된 클라이언트의 버전을 전달한다. AP는 클라이언트의 업데이트가 필요할 경우 PS의 정보를 전달한다.

3.3.3 DCAS PS - DCAS 호스트 상호 인증

(1) [그림 6]과 같이 DCAS AP와 DCAS 호스트의 상호인증이 완료된 후에 DCAS PS와 DCAS 호스트의 상호인증이 수행된다. 이는 DCAS PS가 DCAS 호스트를 Challenge-Response 방식으로 인증하는 것으로 한다

(2) DCAS PS는 DCAS AP로부터 전달 받은 TK를 이용해서 다운로드 되는 DCAS 클라이언트를 암호화하는데 사용될 세션

키(SK)를 암호화하여 DCAS 호스트에게 전송한다. 이 때, DCAS 호스트 인증을 위한 Challenge 값인 Rand3이 함께 전송된다.

(3) DCAS Host는 DCAS PS가 전송한 메시지를 복호화하여 약속된 메시지(SUCCESS)가 포함되어 있으면 TK를 소지하고 있는 정당한 DCAS PS로 간주한다. 이후 획득한 Rand3과 SK를 이용해서 Response를 생성해 DCAS PS에게 전달한다.

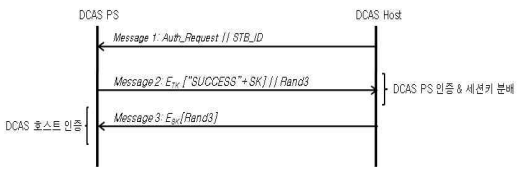
DCAS PS는 DCAS 호스트가 전송한 메시지를 확인함으로써 인증을 완료한다.

3.3.4 DCAS 서버 구성요소간 상호 인증 및 보안 통신

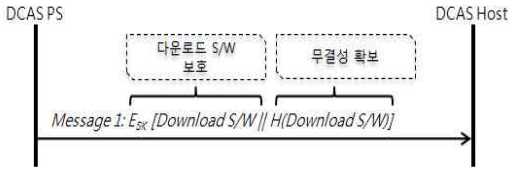
DCAS 서버 구성요소 가운데 DCAS AP와 LKS, DCAS AP와 DCAS PS, DCAS AP와 DPS는 각각 상호인증이 필요하다. DCAS 서버 구성요소는 오픈케이블 규격에서 SSL 지원이 가능하도록 되어 있기 때문에 SSL을 이용해서 상호인증을 수행하는 것으로 한다. 이 때, DCAS PS는 DCAS 호스트에게 DCAS 클라이언트를 다운로드 할 때, DCAS 클라이언트를 보호기 위한 암호키가 필요하다. 이는 DCAS AP가 SSL 채널을 통해서 DCAP PS에게 전달하도록 한다.

3.3.5 다운로드 소프트웨어 보호

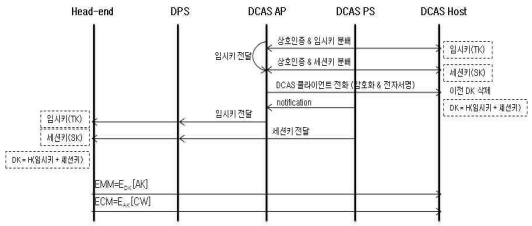
DCAS PS는 [그림 6]에서 분배된 SK를 이용해서 [그림 7]처럼 ESK[DCAS 클라이언트]와 같이 DCAS 클라이언트 프로그램을 암호화하여 DCAS 호스트에게 전달한다. 이때, DCAS PS의 전자서명 없이 무결성 확인을 위한 해쉬값과 암호화된 DCAS 클라이언트만을 전송하는데 이는 이미 PS에 대한 인증이 완료되었기 때문에 묵시적으로 코드에 대한 신뢰성을 확보할 수 있기 때문에 가능하다. 또한 전자서명을 수행하지 않음으로 많은 처리 시간을 필요로 하는 공개키 연산을 최소화할 수 있다.



[그림 6] DCAS PS - DCAS 호스트 상호인증



[그림 7] 다운로드 소프트웨어 보호



[그림 8] DK의 분배

3.3.6 분배키 배포

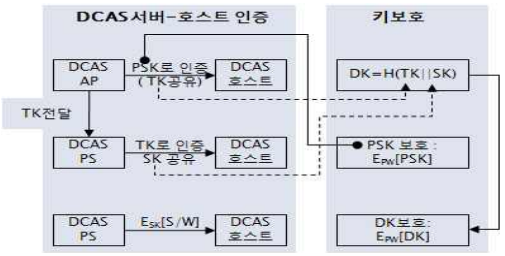
만약 DCAS 클라이언트가 다운로드 되면 DK가 갱신되어야 한다. 이는 DCAS 클라이언트의 갱신이 DK 유출을 포함해서 DCAS 클라이언트에 문제가 발생하는 경우에 이루어지기 때문이다. DK 갱신을 DCAS 호스트와 방송 시스템(Head-end)에서 이루어져 하며, 그 과정은 [그림 8]과 같다.

DCAS 호스트는 DCAS AP 및 DCAS PS와 상호인증을 수행하는 과정에서 획득한 TK와 SK를 이용해서 DK를 생성하고, 이전 DK를 삭제한다. 한 편, DCAS AP와 DCAS PS는 각각 TK와 SK를 Head-end에 전달하고 Head-End는 DCAS 호스트와 마찬가지로 TK와 SK의 해쉬 결과를 DK로 한다.

3.3.7 키 관리

본 논문에서 제안하는 안전한 DCAS 시스템은 인증 및 DCAS 클라이언트 보호를 위해 다양한 키를 사용한다. 안전한 DCAS 시스템 내에서 사용되는 키들의 관계를 살펴보면 [그림 9]와 같다.

우선 방송 콘텐트의 디스크램블링에 사용되는 DK, AK, CW는 일반적인 제한수신 시스템과 동일하다. 이 때, DK는 사용자의 패스워드로 암호화되어 저장된다. DCAS 서버와 DCAS 호스트의 인증에서 가장 기본이 되는 키는 PSK는 온라인으로 배포될 수 없다.

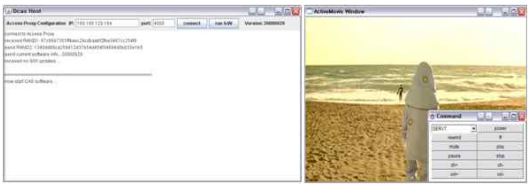


[그림 9] 키 구조

이에 따라 PSK는 DCAS 호스트의 최초 구동을 위해서 입력이 되는 라이선스 키의 해쉬값으로 설정한다. PSK는 사용자가 입력하는 패스워드로 암호화되어 저장된다. DCAS PS와 DCAS 호스트는 PSK로 상호인증을 하는 과정에서 공유되는 TK로 인증을 수행하여 이 과정에서 SK를 공유한다. SK는 다운로드 되는 DCAS 클라이언트를 보호하는데 사용되며 따라서 SK를 통해서 DK를 보호하게 된다.

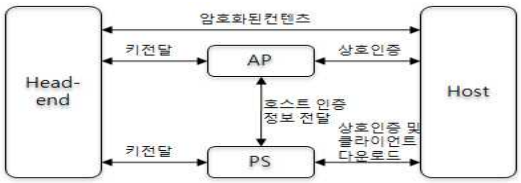
IV. 안전한 DCAS 시스템 구현 및 고찰

본 장에서는 위에 제안한 내용을 바탕으로 [그림 10]과 같이 구현한 안전한 DCAS 시스템을 소개한다.



[그림 10] DCAS 호스트 구동 화면 및 다운로드된 소프트웨어 구동화면

구현된 DCAS 시스템은 DCAS 호스트, DCAS AP, DCAS PS로 실제 DCAS 클라이언트 다운로드에 관여하지 않는 LKS와 DPS는 구현 범위에서 제외하였다. 또한 Head-end에 해당되는 방송 시스템을 대신하여 리눅스 서버가 저장된 동영상 파일을 전송하도록 구현하였다. 따라서 전체 시스템 구성은 [그림 11]과 같다.



[그림 11] DCAS 구현 시스템 전체 구조

4.1 개발환경

개발환경은 [표 1]과 같이 DCAS 호스트의 경우 윈도우를 기반으로 Java TV API를 이용하여 작성하였다. 또한 DCAS AP와 DCAS PS의 경우 리눅스 기반으로 OpenSSL을 이용하여 작성하였다.

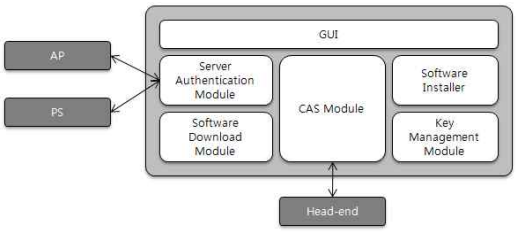
[표 1] 개발 환경

	DCAS 호스트	DCAS AP	DCAS PS
운영체제	Windows XP	Linux	Linux
개발언어	Java(JDK 1.4)	C	C
라이브러리	Java TV API RI 1.1 PJEE 3.1	OpenSSL 0.9.8g	OpenSSL 0.9.8g

4.2 시스템 구조

4.2.1 DCAS 호스트

DCAS 호스트의 구조는 [그림 12]와 같다.



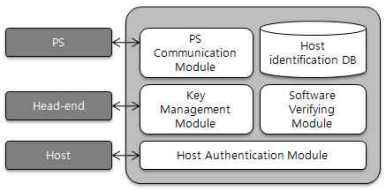
[그림 12] DCAS Host 구조

각각의 모듈은 아래와 같은 기능을 갖는다.

- Server Authentication Module : DCAS AP 및 PS 와의 인증을 수행한다.
- Software Download Module : DCAS S/W를 다운로드하고 검증하는 작업을 수행한다.
- Software Installer : DCAS S/W를 설치하는 작업을 수행한다.
- Key Management : PSK, AK, DK 등의 키 정보를 관리한다.

4.2.2 DCAS AP

DCAS AP의 구조는 [그림 13]과 같다.



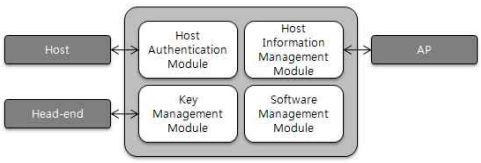
[그림 13] DCAS AP 구조

각각의 모듈은 아래와 같은 기능을 갖는다.

- Host Authentication Module : DCAS Host 인증을 담당한다.
- Host Identification DB : Host의 정보(PSK 등)를 저장한다.
- PS Communicatino Module : TK 전달을 위하여 PS와 통신을 담당한다.
- Key Management Module : Host와 분배하는 키 관리를 담당한다.
- Software Verifying Module : Host에 현재 설치된 소프트웨어를 검증한다.

4.2.3 DCAS PS

DCAS PS의 구조는 [그림 14]와 같다.



[그림 14] DCAS PS 구조

각각의 모듈은 아래와 같은 기능을 갖는다.

- Host Authentication Module : 호스트 인증을 담당한다.
- Key Management Module : TK 저장 및 SK 분배 등의 키 관리 작업을 수행한다.
- Software Management Module : Host로 전송할 S/W를 관리하는 역할을 수행한다.
- Host Information Management Module : AP로부터 전달받은 Host의 정보를 저장한다.

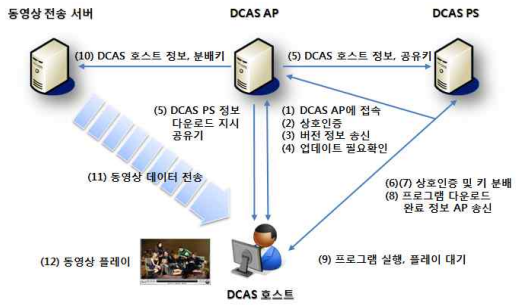
4.3 구현 시스템 기본 동작 과정

구현 시스템의 기본 적인 동작 과정은 [그림 15]와 같이 실행된다.

(1) DCAS 호스트는 미리 설정되어 있는 DCAS AP의 IP 주소 및 포트 정보를 이용하여 DCAS AP에 접속한다.

(2) DCAS AP와 DCAS 호스트는 미리 공유되어 있는 PSK를 이용하여 서로간의 인증을 수행한다.

(3) DCAS 호스트는 자신의 소프트웨어 버전 정보를 DCAS AP로 송신한다.



[그림 15] 구현시스템 동작 과정

(4) DCAS AP는 버전 정보를 통해 업데이트 필요 유/무를 판단한다.

(5) DCAS AP는 DCAS 호스트의 프로그램 업데이트가 필요하다고 판단시 DCAS PS에게 DCAS 호스트의 정보 및 공유키를 전달한다. 또한 DCAS 호스트에게 DCAS PS 접속에 필요한 정보를 송신하고 다운로드를 송신한다.

(6) DCAS 호스트는 수신한 정보를 바탕으로 DCAS PS에 접속 및 상호인증을 수행한다.

(7) DCAS PS는 상호인증 완료시 프로그램을 암호화 하기 위한 키 분배를 수행한다.

(8) DCAS 호스트는 프로그램을 수신 및 복호화하여 설치한뒤 완료 정보를 DCAS AP에게 알린다.

(9) DCAS 호스트는 프로그램을 실행하고 동영상 수신 및 플레이를 대기한다.

(10) DCAS AP는 동영상 전송 서버로 분배키 및 DCAS 호스트 정보를 전달한다.

(11) 동영상 전송 서버는 수신한 정보를 바탕으로 DCAS 호스트에게 암호화된 동영상 데이터를 전송한다.

DCAS 호스트틀 수신한 동영상 데이터를 복호화 및 플레이한다.

4.4 구현 시스템 고찰

4.4.1 보안 문제점의 해소

Ⅲ장에서 도출한 기존 DCAS 시스템의 보안 취약성에 대해서 본 논문에서 제안한 DCAS 시스템의 안전성을 살펴보면 다음과 같다.

① DCAS 서버와 호스트의 상호 인증

DCAS 서버와 호스트간의 불명확한 인증 메커니즘에 대하여 AP와 호스트, PS와 호스트 모두 Challenge-Response 방식을 사용하여 상호 인증을 수행하도록 하였다. AP와 호스트 인증의 경우, 암호 알고리즘으로 스트림 사이퍼가 사용될 경우를 고려하여 미리 분배된 공유키를 분리하여 DCAS AP와 DCAS 호스트가 Reponse를 생성하는데 사용하는 키를 구분하였다. 이때 PS와 호스트 인증에 필요한 키를 분배하여 PS와 호스트의 인증 과정을 명확히 함으로서 DCAS PS 혹은 DCAS 호스트 위장 공격에 대비하였다.

② DCAS 클라이언트의 보호

4.1.1에서와 같이 DCAS PS 또는 DCAS 호스트로 위장하는 공격에 대비함으로서 잘못된 클라이언트를 다운로드 받는것을 방지하였다. 또한 클라이언트의 전송 시 SK를 사용하여 암호화를 함으로서 소스코드의 노출을 막아 역공학 방법 등을 사용하여 발생될 수 있는 위험을 제거하였다. 이때 사용되는 암호화 키 또한 DCAS PS와 DCAS 호스트의 상호 인증 후 기밀성이 보장된 채널을 통하여 전송된다. 해쉬 값 또한 클라이언트와 같이 전송하도록 하여 무결성 또한 확보하였다.

4.4.2 키 분배 및 관리

DCAS AP와 DCAS 호스트의 인증 후 기밀성이 보장된 채널을 통하여 DCAS PS와 DCAS 호스트 인증에 사용되는 키를 분배하였다. 또한 DCAS AP와 DCAS 호스트 간 분배된 키와 DCAS PS와 DCAS 호스트간 분배된 키를 조합하여 CAS에 사용되는 DK 분배 문제를 해결하였다. DK는 DCAS 클라이언트가 업데이트 될 때마다 이를 통해서 미리 분배된 공유키가 DCAS AP 및 DCAS 호스트 외부로 방출되는 경우를 제거하고 사용횟수를 최소화하여 공유키(PSK)의 유출 위협을 최소화 하였다. 이 과정에서 PS와 호스트 인증에 사용되는 키를 분배하도록 함으로서 PS와 호스트 인증에 필요한 초기 키 분배 문제도 해결하였다.

4.4.3 네트워크 보안 요구사항의 만족

본 논문에서 제안한 DCAS 시스템은 앞서 도출한 네트워크 보안 요구사항을 다음과 같이 만족한다.

- 요구사항 1~5: 이는 시스템 요구사항에 속하는 것으로써 본 논문에서는 다루지 않는다.

- 요구사항 6: DCAS AP와 DCAS 호스트는 Challenge-Response 기반의 상호인증을 수행한다. 이 때, 전송 방향에 따라 서로 다른 키를 사용함으로써 키 스트림 재사용 공격을 방지한다. 그리고 해쉬함수를 이용하여 메시지 재전송 공격을 방지한다.
- 요구사항 7: DCAS PS와 DCAS 호스트는 Challenge-Response 기반의 상호인증을 수행한다. 이 때, DCAS 호스트에 의한 DCAS PS 인증은 DCAS PS가 DCAS 호스트와 DCAS AP가 공유하고 있는 키를 소지하고 있는지를 확인하는 것으로 이루어진다.
- 요구사항 8: DCAS AP와 DCAS LKS는 SSL 통신을 수행하도록 하였다. 따라서 SSL을 통해서 DCAS AP와 DCAS LKS 간의 상호인증이 이루어진다.
- 요구사항 9: DCAS AP와 DPS 역시 SSL 기반의 상호인증을 수행하도록 하였다.
- 요구사항 10: DCASP AP와 DCAS PS는 SSL 기반의 상호인증을 수행하도록 하였다.
- 요구사항 11: DCAS LKS에게 DCAS AP와 TA와의 통신 이외에 다른 통신은 허용되지 않는다.
- 요구사항 12: 그림 4에서 보는 바와 같이 DPS는 DCAS AP와의 통신만 허용되도록 DCAS 시스템을 설계하였다.
- 요구사항 13: 그림 4에서 보는 바와 같이 DCAS PS는 DCAS AP와의 통신만 허용된다.
- 요구사항 14: DCAS AP와 DCAS LKS 간의 통신 내용은 SSL을 통해 보호되도록 설계하였다.
- 요구사항 15: DCAS AP와 DPS와의 통신 내용 역시 SSL을 통해서 보호되도록 설계하였다.
- 요구사항 16: DCAS AP와 DCAS PS 간의 통신 내용은 SSL을 통해서 기밀성이 무결성이 보장되도록 하였으며, 전자서명을 통해 메시지 인증이 이루어지도록 하였다.
- 요구사항 17: DCAS PS와 DCAS 호스트 간의 통신 내용은 DCAS PS와 DCAS 호스트가 상호인증 과정에서 분배한 키 SK를 통해서 보호된다.

위와 같이 제안한 DCAS 보안 프레임워크는 도출된 보안 요구사항을 모두 만족하며, 안전하고 신뢰할 수 있는 방법으로 DCAS 클라이언트의 다운로드를 수행함을 알 수 있다.

V. 결 론

최근의 방송과 통신의 융합 시대에서 소프트웨어 기반의 제한수신 시스템인 DCAS 시스템은 우수한 호환성, 간단하고 편리한 CAS 클라이언트의 업데이트, DRM 등 다른 서비스와의 우수한 연동성 등 여러 가지 장점을 갖고 있어 빠른 활성화가 기대된다.

하지만 DCAS 시스템이 활성화되기 위해서는 기존 인터넷환경이 가지고 있는 여러 가지 보안 문제를 반드시 해결해야 한다. 그러나 현재 OpenCable에서 표준화를 진행하고 있는 DCAS 시스템에서는 보안 서비스와 관련한 연구 및 개발이 더디게 진행되고 있는 실정이다.

이에 본 논문에서는 다운로드 되는 DCAS 클라이언트를 보호할 수 있는 안전한 DCAS 시스템을 제안하였다. 기존 DCAS 시스템은 DCAS 서버와 호스트 간의 상호인증 결여로 인한 위장 공격, 프로그램 다운로드시 DCAS 클라이언트 보안의 취약성, DCAS 서버 구성요소 간의 상호인증 부재 등의 문제가 있다. 본 논문에서는 이와 같은 문제를 해결하기 위해 네트워크 보안 요구사항을 도출하고 이를 만족할 수 있는 상호인증 및 클라이언트 보호 방안을 제안 및 구현하였다. 따라서 본 논문의 내용이 앞으로 진행될 Opencable DCAS 표준화의 보안 부분에 많은 기여를 할 수 있을 것으로 기대된다.

앞으로 본 논문에서 제안한 방안과 더불어 최초 CAS 내에 저장되어 분배되는 공유키 및 분배키 등의 정보를 시스템 측면에서 안전하게 보호할 수 있는 연구 및 개발이 지속적으로 이루어진다면 IPTV의 활성화가 보다 빨리 실행 될 수 있을 것으로 전망된다.

참 고 문 헌

[1] 권호영, IPTV의 동향과 전략, 커뮤니케이션북스, 2004년 12월.

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

[3] N. Borisov, I. Goldverg, and D. Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11,” Proceeding of the 7th Annual International Conference on Mobile Computing and Networking, pp. 180-189, July 2001.

[4] OpenCable, “OC-SP-CDL2.0-I06-080118:

Common Download 2.0," OpenCable Specification, Jan. 2008.
[5] OpenCable, "OC-SP-DCAS-CP-D01-060206: OpenCable DCAS Content Protection Specification," OpenCable Specification, Feb. 2006.
[6] 전한얼, 이윤경, 최진용, 허민성, 이현석, "방송통신 기술동향연구," 방송위원회 연구센터, 2007년 1월.
[7] ETSI TS 103 197 v1.4.1, "Digital Video Broadcasting(DVB) Head-end Implementation of DVB," Simulcrypt, Dec. 2004.
[8] ETSI Technical Report 289, "Support for use of scrambling and Conditional Access within digital broadcasting system," Oct. 1996.
[9] OpenCable, "OC-TR-DCAS-D01-060206: DCAS System Overview Technical Report," OpenCable Technical Report, Feb. 2006.
[10] OpenCable, "OC-SP-HOST2.5-CFR-D01-060206: OpenCable DCAS Host Device 2.5 core Functional Requirements," OpenCable Specification, Feb. 2006.
[11] ATIS, "IIF Default Scrambling Algorithm(IDSA) IPTV Interoperability Specification," ATIS-0800006, Mar. 2007.
[12] ITU-T, "Functional Requirements and Architecture for IPTV Security Aspects," X.iptvsec-1, May 2008.
[13] ATSC, "Advanced Common Application Platform," http://www.atsc.org/standards/a101.html
[14] CableLabs, "The OpenCable Application Platform," http://www.opencable.com/ ocap/

<著者紹介>

강 성 구 (Seong-Ku Kang) 학생회원
2008년 2월: 충남대학교 컴퓨터공학과 졸업
2008년 3월 ~ 현재: 충남대학교 컴퓨터공학과 석사과정
<관심분야> IPTV 보안, 네트워크 보안, 암호프로토콜

박 종 열 (Jong-Youl Park) 정회원
1996년 8월: 충남대학교 컴퓨터공학과 공학사
1999년 2월: 광주과학기술원 정보통신공학과 공학석사
2004년 8월: 광주과학기술원 정보통신공학과 공학박사
2001년 8월: U. of Utah, School of Computing 초빙연구원
2004년 7월 ~ 현재: 한국전자통신연구원 선임연구원
<관심분야> 방송 수신 제한 시스템, 전자지불, 인증시스템, 분산 시스템

백 의 현 (Eui-Hyun Paik) 정회원
1984년 2월: 숭실대학교 전산학과 학사
1987년 2월: 숭실대학교 전산학과 석사
1997년 2월: 숭실대학교 전산학과 박사
1987년 2월 ~ 현재: 한국전자통신연구원 책임연구원
<관심분야> IPTV, 방송 수신 제한, 개방형 홈네트워크, 상황인지

박 춘 식 (Choon-Sik Park) 종신회원
1995년: 일본동경공업대학 공학박사
1982년 ~ 1999년: 한국전자통신연구원 책임연구원
2000년 ~ 2008년: 국가보안기술연구소 책임연구원
2009년 ~ 현재: 서울여자대학교 정보보호전공 교수
<관심분야> 암호이론, 정보이론, 네트워크보안

류 재 철 (Jae-Cheol Ryou) 종신회원
1988년 5월: Iowa State University 전산학과 석사
1990년 12월: Northwestern University 전산학과 박사
1991년 ~ 현재: 충남대학교 정보통신공학부 교수
1997년 ~ 현재: 한국정보보호학회 이사
2001년 ~ 현재: 국가정보원 정보보호시스템 인증위원회 위원
2003년 ~ 현재: 인터넷침해대응기술연구센터 센터장
<관심분야> IPTV 보안, 인증이론 및 시스템, 유·무선 인터넷 보안