情報保護學會論文誌
第13券 第1號, 2003. 2

디지탈 컨텐츠 배포를 위한 보안 체계에 관한 연구

김 대 엽*, 주 학 수**

A Study on Security Architecture for Digital Content Dissemination

Dae-Youb Kim*, Hak-Soo Ju**

요 약

인터넷 인프라의 보급과 이용인구의 급속한 증가는 off-line을 통해서 물리적으로 제공받아 이용하던 다양한 정보와 자료, 그리고 디지탈 컨텐츠를 인터넷을 통해서 쉽고 빠르게 이용할 수 있는 서비스의 기반이 되고 있다. 그러나 인터넷 서비스를 통해서 제공되는 다양한 컨텐츠의 저작권 보호와 불법 복제 등과 같은 문제는 해당 사업의 발전을 저해하는 위험요소가 되고 있다. 이와 같은 문제를 해결하기 위한 방안으로 컨텐츠를 이용할 수 있는 정당한 자격을 소유한 사용자만이 해당 컨텐츠를 정상적으로 이용할 수 있도록 하는 접근제어(Access Control, AC) 기술이 연구되고 있다. 위성 방송에서 사용되고 있는 제한수신 시스템(Conditional Access System, CAS)과 인터넷 컨텐츠 서비스에 사용되고 있는 디지탈 저작권 관리 시스템(Digtal Right Management System, DRMS)은 현재 상용화되어 있는 AC의 대표적인 모델이라 할 수 있다. CAS와 DRMS는 지불 구조에 기반을 둔 형태(Payment Based Type, PBT)의 AC 기술이라 할 수 있다. 본 논문에서는 [5]에서 제시된 지불 구조에 독립적인 형태(Payment Free Type, PFT)의 AC를 위한 보안 체계를 살펴보고, 각각의 특징을 간략하게 정리한다. 또한 효과적인 운영을 위한 PFT 기반의 새로운 AC 구조를 제시한다.

ABSTRACT

The diffusion of internet infrastructure and a fast increase of population to use it is becoming a base of the service that can use various information, data and digital contents which were provided through off-line physically and used. Recently, the techniques for copy deterrence and copyright protection have been important in e-commerce because various contents in digital form can be duplicated easily.

The Access Control(AC) technique that only a user having the qualifications can access and use contents normally has been studied. The Conditional Access System(CAS) used in a satellite broadcasting and Digital Right Management System(DRMS) used for contents service are representative models of current commercialized access control. The CAS and DRM can be considered as an access control technique based on the payment based type(PBT). This paper describe the access control method of payment free type(PFT) suggested in [5] which are independent on the payment structure. And then we suggest a new access control method of payment free type which is more efficient than the previous one.

Keyword : *DRM, CAS, 컨텐츠 보호*

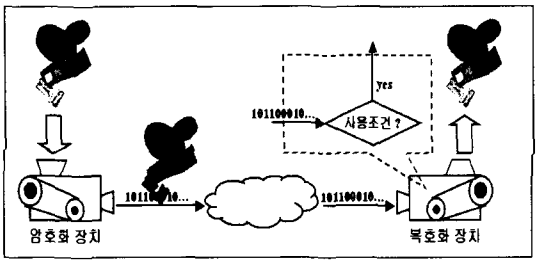
Ⅰ. 서 론

인터넷 이용인구의 급속한 증가와 인프라의 보급, 그리고 위성, 케이블 등을 이용한 다양한 전송 매체의 발달은 기존의 off-line을 통해서 물리적으로 이용하던 정보와 자료(이하, 컨텐츠)를 사용자들이 on-line

* 삼성 종합기술원, i-Networking Lab.(daeyoub.kim@samsung.com)
** 한국정보보호진흥원(hsju@kisa.or.kr)

이나 무선 환경을 통해서 쉽게 이용할 수 있도록 서비스를 제공하는 기반이 되고 있다. 또한 이와 같은 서비스는 각종 무선 단말기와 무선 인터넷이 보급으로 서비스의 종류 뿐 아니라 이용자 수도 급속히 증가할 것으로 예상된다. 그러나 이러한 서비스를 지속적으로 제공하고, 컨텐츠의 질을 높이기 위해서는 사용자 인증 및 개인 정보 보호, 그리고 저작권자의 권리 보호와 유료서비스를 통한 효과적인 이용료 징수 등의 문제가 함께 해결되어야 한다. 특히, 컨텐츠의 불법 복사와 배포, 그리고 변조와 같은 불법 이용은 저작권자와 서비스 사업자의 재산권을 침해하고 경제적으로 막대한 피해를 입혀서, 해당 서비스 사업의 발전을 저해하는 요소가 될 수 있다. 또한 저작권 침해 사고는 컨텐츠 제작자의 창작의욕을 떨어뜨려서 장기적으로 컨텐츠의 고급화를 지향하는 소비자의 욕구를 충족시킬 수 없게 되어 컨텐츠 서비스의 발전을 가로막는 요소가 될 수 있다. 그러므로 저작권자와 사업자의 권리를 보호할 수 있는 장치의 개발이 필수적이라 하겠다.

디지탈 컨텐츠에 대한 접근제어(Access Control, AC) 기술은 저작권 보호와 컨텐츠의 유료 서비스를 제공하기 위하여 사용되는 방법 중 하나로 많은 연구가 진행되었으며, 현재 다양한 형태의 상용화 제품들이 개발되고 있다. 컨텐츠 접근제어 시스템이란 사업자가 제공하는 컨텐츠에 대하여 해당 사업자가 정당한 자격 또는 권한을 부여한 사용자만이 컨텐츠를 정상적으로 이용할 수 있도록 제어하는 시스템을 의미한다. [그림 1]에서 볼 수 있는 것처럼, 기본적으로 접근제어 시스템은 사업자가 제공하는 컨텐츠를 암호화해서 사용자에게 전달하고, 사용자가 암호화된 컨텐츠를 복호화 할 때 특정 조건에 부합된 사용자만 정상적으로 복호화를 수행할 수 있도록 제어한다. 복호화에 필요한 조건은 서비스 사업자 또는 인증 시스템을 통해서 각각의 사용자에게 안전하게 전달/관리된다. 접근제어 기술을 이용한 유료 컨텐츠 서비스의 대표적인 시스템으로 위성방송 시스템에 사용되고 있는 제한 수신 시스템(Conditional Access System, CAS)과 유/무선 인터넷 컨텐츠 서비스에 사용되는 디지털 저작권 관리 시스템(Digital Right Management System, DRMS)을 들 수 있다.



〔그림 1〕 컨텐츠 AC 기술

CAS는 위성 및 케이블을 통해서 전송되는 디지털 방송 프로그램 및 데이터를 스크램블 키(Control Word)를 사용해서 스크램블(Scramble)한 후, 가입자에게 스크램블 된 프로그램을 제공한다. 해당 프로그램에 대한 정당한 시청 권한*(Entitlement)*을 소유한 수신자만이 스크램블에 사용된 키를 제공받아 프로그램을 디스크램블(Descramble)해서 이용할 수 있도록 제어하는 시스템을 의미한다. 이와 같은 서비스를 안전하게 제공하기 위해서 CAS에서는 암호화 장치인 스크램블러와 복호화 장치인 디스크램블러, 그리고 가입자의 자격을 저장/관리하는 가입자 스마트카드 등을 사용하며, 효과적인 가입자 자격 제어를 위하여 일반적으로 시청 자격 제어 메시지(Entitlement Control Message, ECM)와 가입자 자격 관리 메시지(Entitlement Management Message, EMM)를 사용한다[1~3].

DRMS는 저작권자의 권리를 보호하고, 컨텐츠의 불법 사용을 막기 위해 정당한 이용 권한(License)을 할당받은 사용자만이 허용된 규칙에 따라 컨텐츠를 사용하도록 지원하고, 불법적인 접근과 사용을 방지하는 시스템이다. 즉, 적법하게 라이선스(License)를 발급 받은 사용자만이 라이선스가 허용하는 사용규칙에 따라 해당 컨텐츠를 이용할 수 있도록 제어한다. 이와 같은 서비스를 제공하기 위하여 DRMS에서는 사용자에게 제공되는 응용 프로그램(Virtural Machine, VM)과 라이선스를 이용한다. 제공되는 컨텐츠와 라이선스는 암호화된 상태로 사용자에게 전달되며, 사용자 VM을 통하여 복호화와 확인 과정을 거쳐서 이용하게 된다[4~6].

CAS와 DRMS는 프로그램이나 컨텐츠의 사용료를 효과적으로 징수할 수 있도록 설계된 Payment-Base Type(PBT)의 접근제어 구조를 갖는다면, 지불 구조에 독립적인 접근제어 형태인 Payment-Free Type(PFT)를 고려해 볼 수 있다. PBT에서 디지털 컨텐츠의 배포 및 사용은 해당 컨텐츠의 접근 및 사용에 따른 요금 정책을 기본으로 전체 시스템을 제어한다. 즉, 모든 디지털 컨텐츠에는 대응되는 사용료와 관련된 정보가 할당되고, 이 정보에 따라서 정당한 값을 지불하고 해당 컨텐츠에 대한 접근 및 사용 권리를 소유한 사람만이 컨텐츠를 이용할 수 있다. PFT에서는 시스템

구성 요소들의 신뢰성과 보안과 관련된 요소를 기본으로 컨텐츠의 접근 및 사용을 제어한다. 그러나 Payment Gateway나 다른 지불과 관련된 시스템과 연계해서 상업적인 서비스에 충분히 이용할 수 있다.

이와 같은 PBT 또는 PFT AC 구조의 설계에 있어서 반드시 고려되어야 하는 것은 안전성과 효율성 뿐 아니라 사용자 편리성이다. 특히, AC를 실제 상용 서비스에 적용하기 위해서는 사용자 편리성이 중요하게 고려되어야 한다. 본 논문에서 우리는 먼저 [7]에서 제시된 PFT 관점에서 보안 체계(Security Architecture)를 살펴보고, 그 특징을 간략하게 설명하겠다. 또한 효율성과 편리성을 증가시킬 수 있는 새로운 구조의 AC 방안을 제시하도록 하겠다.

본 논문의 목적은 새로운 AC 구조의 제안에 둔다. 그러므로 제시된 구조의 구체적인 안전성 문제는 시스템 설계 및 구현에 관한 문제로, 본 논문의 범위를 벗어나는 것으로 간주하여 자세히 다루지 않고, 대략적인 필요성만 설명하기로 한다.

II. 본 론

2.1 Security Architecture

이 절에서는 [7]에서 제시된 보안 체계에 관하여 살펴보고, 그 특징을 알아본다.

2.1.1 구성 요소

[7]에서 제시된 보안 체계를 구분하는 세 가지 요소는 다음과 같다:

- 응용프로그램(Virtual Machine, VM)
- 사용 규칙(Control Set, CS)
- 컨텐츠 배포 형식(Distribution Style)

응용프로그램(VM)은 사용자의 컴퓨터 또는 수신기에서 사용되는 S/W로 디지탈 컨텐츠 이용을 위한 기능과 컨텐츠 접근 및 이용을 제어하기 위한 기능이 탑재되어 있다. 일반적으로 디지털 컨텐츠는 접근 제어를 위하여 암호화나 다른 보안기술을 이용해서 캡슐화(encapsulation)된 상태로 사용자에게 제공된다. 이처럼 캡슐화된 컨텐츠는 배포자(Distributor) 또는 인증 센터(Control Center)가 제공한 특정 VM을 통해서만 접근할 수 있다.

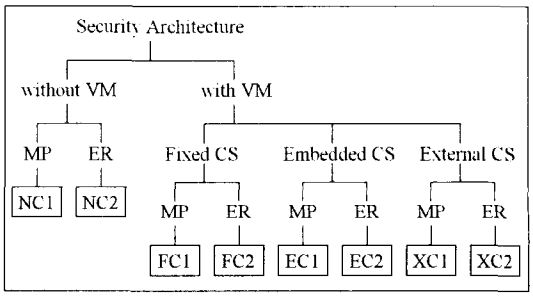
사용 규칙(CS)은 컨텐츠에 대한 접근 권한이나 이용 규칙을 명시한 목록으로 사용자의 컨텐츠 접근과 이용을 제어하기 위하여 VM에서 사용된다. VM은 캡슐화된 컨텐츠의 정보와 사용 규칙에 명시된 정보를 비교해서, 해당 컨텐츠의 접근 및 이용 가능여부를 결정하게 된다. [7]에서는 CS를 크게 Fixed Control Set, Embedded Control Set, External Control Set으로 구분하고 있다.

배포 형식은 서비스 사업자가 디지탈 컨텐츠를 사용자에게 전달하는 형식을 의미한다. [7]에서는 배포 형식을 Message Push(MP)와 External Repository(ER)로 나눠서 고려하고 있다. MP 환경에서 사용자가 특정 컨텐츠를 선택하고, 해당 컨텐츠를 요청하면 배포자는 각각의 사용자에게 해당 컨텐츠를 직접 전송한다. ER환경 아래에서는 네트웍 상에 있는 컨텐츠 배포 서버(Repository Server, RS)를 두고, 배포자나 사업자가 RS에 컨텐츠를 등록한다. 사용자는 RS에 접속한 후 컨텐츠를 직접 다운로드받아서 이용한다.

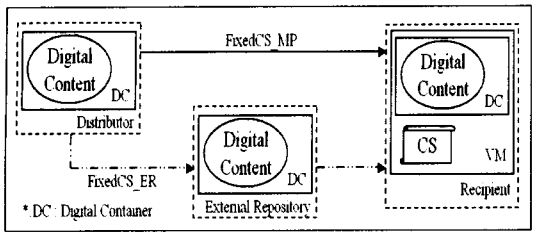
2.1.2 Security Architectures와 특징

[그림 2]는 [7]에서 제시된 보안 체계를 요약한 것이다. 제시된 구조는 사용자 측면에서 VM의 필요여부에 따라 'without VM'(이하, w/oVM)과 'with VM'(이하, wVM) 두 가지 종류로 구분된다. wVM을 사용하는 경우는 다시 CS 제공 형태와 이용 방법에 따라 Fixed CS, Embeded CS, 그리고 External CS 세 종류로 구분된다. 또한, 모든 형태의 AC는 컨텐츠 배포 형식에 따라 각각 MP와 ER로 세분화된다.

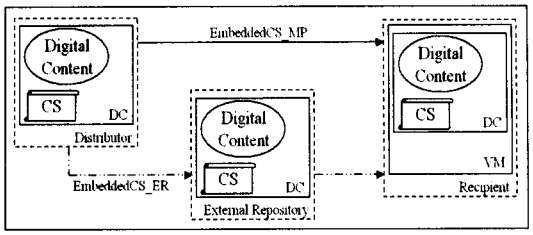
컨텐츠는 접근 제어를 위하여 캡슐화 된 상태로 배포되는데, 이와 같이 캡슐화 과정을 거쳐 생성된 결과를 디지탈 컨테이너(Digital Container, DC)라고 부른다. VM을 사용하지 않는 AC 구조(without VM, w/oVM)의 경우, 사용자 측면에서 DC를 열 수 있는 도구가 사용자에게 없기 때문에 컨텐츠는 캡슐화 과정을 거치지 않고 배포된다. 즉, 암호화되지 않은 상태로 전



[그림 2] 컨텐츠 보안 체계



〔그림 3〕 Fixed CS

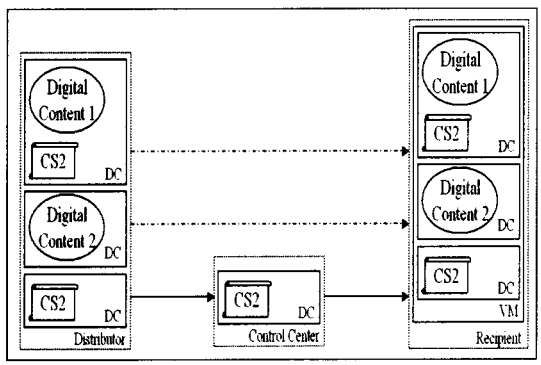


〔그림 4〕 Embedded CS

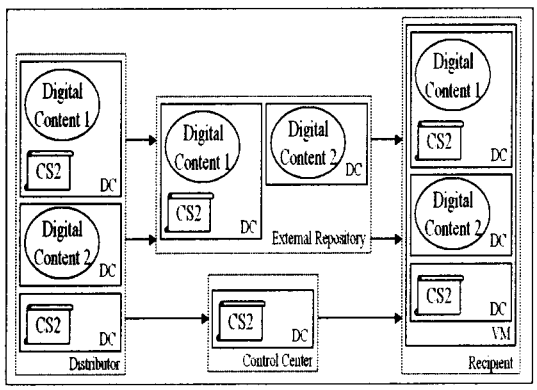
송된다. 이 경우, 컨텐츠가 배포된 이후에 해당 컨텐츠에 대한 접근 및 사용을 직접적으로 제어할 수 있는 방법이 없다. 그러므로, 해당 컨텐츠에 대한 불법적인 복사 및 배포, 변조 등을 막을 수 없기 때문에 상용 서비스나 컨텐츠의 접근 제어를 필요로 하는 서비스에는 이용할 수 없다.

이제 VM을 사용하는 AC의 구조를 살펴보자. [그림 3]은 Fixed CS 형태의 AC 시스템을 설명하고 있다. Fixed CS는 컨텐츠의 접근과 사용을 제어하기 위해 필요한 CS가 VM에 고정된 상태로 포함되고, VM이 배포될 때 함께 사용자에게 전달된다. 그러므로 디지털 컨텐츠에 대응되는 특정 VM이 없이는 해당 컨텐츠를 이용할 수 없다. 접근 제어는 기본적으로 VM과 그 안에 내장된 CS를 통해서 이루어진다. 즉, VM은 내장된 CS의 규칙에 따라 해당 컨텐츠의 이용을 제어한다. Fixed CS 형태의 AC 시스템은 특정 단일 컨텐츠의 배포 및 사용제어에 효과적이고, 서비스 유형에 따라 VM에 복수개의 CS를 내장시킬 수 있기 때문에 컨텐츠 그룹화 서비스를 제공할 수 있다는 장점이 있다. 그러나 CS가 VM에 고정된 상태로 내장되어 배포되기 때문에, 사용자가 컨텐츠 이용을 요청하면 VM을 새로 생성해서 전송해야 되며 배포가 완료된 이후에 CS를 변경하는 것이 어렵다는 단점이 있다. 즉, CS를 변경하기 위해서는 새로운 CS를 포함하는 VM을 생성해서 해당 가입자에게 전달해야 된다. 또한 컨텐츠의 정보가 변경되면, 해당 컨텐츠의 CS를 내장하고 있는 모든 VM을 갱신해야 된다. 이처럼 가입자의 CS 변경 요청이나 컨텐츠 사업자의 컨텐츠 정보 변경 등의 작업은 인증 및 컨텐츠 배급을 담당하는 서버에 많은 작업 양을 요구하기 때문에 다양하고 편리한 컨텐츠 서비스에는 적당하지 못한 구조이다.

Embedded CS 형태의 AC 시스템은 [그림 4]에서 볼 수 있듯이 컨텐츠와 해당 컨텐츠의 CS를 함께 캡슐화 해서 DC를 생성/전송한다. 배포된 컨텐츠에 대한 접근 및 이용 제어는 VM과 DC에 포함된 CS를 통해서 이루어진다. Fixed CS 형태의 AC와 비교해서 Embedded CS의 경우 CS를 VM과 독립적으로 운영할 수 있다는 장점이 있으나 CS가 컨텐츠와 함께 캡슐화 되기 때문에 컨텐츠 그룹화 서비스는 제공할 수 없다. 또한 CS가 컨텐츠의 DC에 내장된 형태로 제공되기 때문에 동일한 컨텐츠를 이용하는 사용자라 하더라도 요청한 이용 규칙이 다를 경우, 각각의 사용자를 위한 DC를 새로 생성해야 되기 때문에 컨텐츠 배급 서버의 작업 양이 증가 할 수 있다. CS를 관리하는 인증기관(Control Center, CC)이 없기 때문에 컨텐츠가 전달된 이후에 배급자는 배포된 컨텐츠에 대한 CS를 변경할 수 없다.



〔그림 5〕 MP 형태의 External CS



〔그림 6〕 ER형태의 External CS

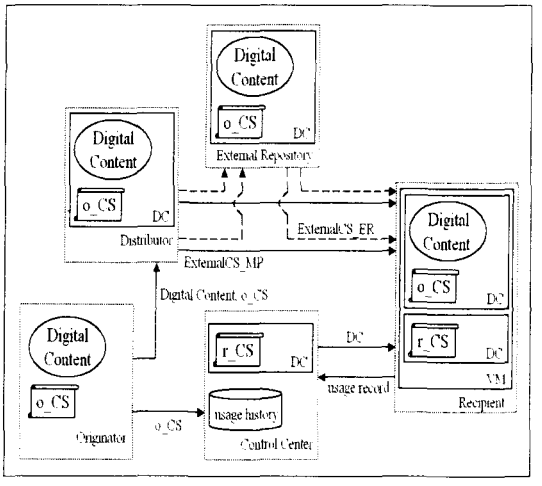
[그림 5]와 [그림 6]에서처럼, External CS 형태의 AC 시스템은 컨텐츠와 해당 컨텐츠를 이용하기 위해 필요한 CS, 그리고 VM을 독립적으로 운영한다. 특히 Fixed CS나 Embedded CS 형태의 AC와는 달리 가입자의 라이선스를 생성하고 배포하는 인증기관(Control Center, CC)을 운영한다. CC는 컨텐츠 배포자와 이용자가 모두 신뢰할 수 있는 기관으로 실제 서비스에서는 CS의 관리 뿐 아니라 사용자의 컨텐츠 사용 이력도 함께 관리한다. 사용자는 컨텐츠와 CS를 배포자와 인증기관을 통해서 각각 획득해야 되기 때문에 컨텐츠에 대응되는 CS를 획득할 수 있는 방법을 알고 있어야 한다. 이와 같은 이유 때문에 일반적으로 컨텐츠를 캡슐화 한 DC는 컨텐츠와 해당 컨텐츠의 기본적인 정보(예를들어 컨텐츠 인증자, CS 획득을 위한 URL, 저작권자 정보 등)로 구성된다.

External CS 형태의 AC에서 사용자의 컨텐츠 이용 권한을 나타내는 CS를 운영하는 방법에는 두 가지 종류가 있다. 첫 번째 방법은 컨텐츠를 획득한 사용자(또는 사용자의 VM)가 해당 컨텐츠의 DC에 포함되어 있는 라이선스 정보(URL)를 이용해서, 라이선스를 발급받을 수 있는 CC에 접속한다. 컨텐츠 이용에 필요한 CS를 CC에 요청하고, 이를 발급 받아 VM을 통해서 컨텐츠를 이용한다. 두 번째 방법은 컨텐츠 배포자가 사용자에게 컨텐츠(예, digital content 1)를 전달할 때 다른 컨텐츠(예, digital content 2) 이용에 필요한 CS(예, CS2)를 함께 전달하는 것이다. 전자의 경우, 사용자는 이용을 원하는 컨텐츠를 먼저 획득하고 DC에 내장된 정보를 이용해서 라이선스를 신청한다. 반면 후자와 같은 형태의 시스템이 MP 환경 아래에서 운영된다면, 사용자가 컨텐츠를 신청할 때 다음에 신청할 컨텐츠의 라이선스를 함께 신청해서 미리 획득해 둔다. 그러나 후자와 같은 형태의 서비스는 실제 운영에 있어 가입자가 컨텐츠를 선택할 때 많은 제약을 받게 될 수 있다. 또한 ER 환경 아래에서 운영된다면, 가입자마다 다른 이용 규칙을 적용하는 것이 불가능하다. 그러므로 전자의 방법이 보편적으로 이용되고 있다. 앞으로 본 논문에서 External CS 형태의 AC는 전자를 의미하는 것으로 한다.

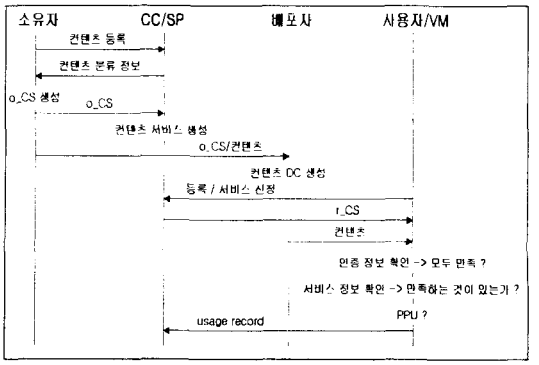
External CS 형태를 갖는 AC는 컨텐츠와 CS를 독립적으로 운영하므로 CS의 변경과 갱신이 용이하다는 장점이 있다. 그러나 컨텐츠 DC를 확보한 이후에, 라이선스 정보에 따라서 CS를 획득하기 때문에 Fixed CS 형태에서 제공되는 컨텐츠 그룹화 서비스를 포함한 다양한 서비스 운영이 어렵다는 단점과 가입자가 컨텐츠와 CS를 획득하기 위하여 두 번의 접속이 필요하다는 불편함이 있다.

2.2 컨텐츠 Access Control 제안

Fixed CS과 Embedded의 경우 CS를 내장한 VM과 컨텐츠 DC가 배포된 이후에 내장된 CS를 변경하는 것이 어렵다. 또한, 모든 사용자에게 동일한 CS를 적용하지 않는다면, 사용자의 요구에 따라 VM과 컨텐츠 DC를 새로 만들어야 되기 때문에 컨텐츠 배포서버에 많은 작업량을 요구한다. External CS의 사용자는 컨텐츠와 대응되는 CS를 함께 획득해야 컨텐츠를 이용할 수 있고, 특히 컨텐츠 DC에 포함되어 있는 CS 획득을 위한 URL을 획득해야 대응되는 CS를 신청할 수 있다. 그러므로 개별 컨텐츠를 선택해야만 이용이 가능하기 때문에 현재 위성방송에서 제공하고 있는 것과 같은 다양한 컨텐츠 서비스를 제공하기



〔그림 7〕 새로운 AC 구조



〔그림 8〕 AC의 운영

어렵고, 사용자의 선택도 제한적일 수밖에 없다.

[7]에서 제시된 VM을 이용한 AC의 경우, 세 종류 CS(Fixed CS, Embedded CS, 그리고 External CS) 형태는 각각의 특징에 따라 유용하게 이용될 수 있다. 그러나 배포된 CS의 변경이 어렵고 다양한 컨텐츠 서비스에 적용하기 어렵다는 단점을 가지고 있다. 이와 같은 문제의 근본적인 원인은 사용자와 VM을 일대일 대응시켜서 사용하거나, 컨텐츠와 CS를 일대일 대응시켜서 사용하는 구조에 있다. 앞서 언급했던 것처럼 이러한 대응 구조에서는 서비스 제공자(Service Provider, SP)나 컨텐츠 제공자(Content Provider, CP)가 자신들이 소유한 컨텐츠를 가지고 컨텐츠 그룹 서비스, 주제 서비스, 예약 서비스, 그리고 Pay-Per-View와 같은 다양한 서비스를 사용자에게 제공하기 어렵다. 뿐만 아니라 off-line 전용 또는 범용 장치를 사용해서 해당 컨텐츠를 이용하려는 사용자에게는 서비스를 제공할 수 없다.

이처럼 기존의 AC 구조들이 갖고 있는 문제점을 해결하고, 서비스/컨텐츠 운영자에 의한 다양한 서비스가 가능하도록 하기 위하여 사용자 CS와 저작권자 CS의 두 종류 CS를 이용한 External CS 형태의 새로운 AC 구조를 제안한다.

2.2.1 Control Set의 구성과 응용

제안하는 AC 구조에서는 컨텐츠 소유권자의 요구사항을 명시한 저작권자 CS(originator CS, o_CS)와 서비스 제공자로부터 컨텐츠를 공급받아 이용하려는 사용자의 접근 및 이용 권한을 나타내는 사용자 CS(recipient CS, r_CS)를 사용해서 컨텐츠의 배포 및 이용을 제어한다. 이와 같은 구조를 운영하기 위해서는 SP의 역할을 담당하는 구성요소가 필요하다. 본 논문에서는 CC가 서비스 사업자 또는 서비스 운영자의 역할을 병행한다고 가정한다. 또한 컨텐츠 DC는 배포자에 의해서 생성된다고 가정하자. 그러나 실제 서비스에서 컨텐츠 DC는 저작권자에 의해서도 생성될 수 있다.

o_CS는 컨텐츠의 저작권자(또는, 소유권자)에 의해서 생성되며, 해당 컨텐츠를 이용하기 위해서 사용자가 충족시켜야 하는 조건들을 나열하기 위하여 사용한다. 사용자가 컨텐츠를 이용하기 위해서는 제공하는 서비스에 따라 o_CS에 명시된 조건들을 전부 또는 일부 만족시켜야 된다.

o_CS의 구성은 크게 컨텐츠 id, 이용 규칙, 그리고 서비스 목록으로 구분된다. 컨텐츠 id는 컨텐츠 고유 식별자로, CC로부터 할당받은 값을 사용한다. 이용 규칙은 해당 컨텐츠를 이용할 수 있는 자격과 범위를 명시하기 위해 사용된다. 예를 들어 해당 컨텐츠를 사용할 수 있는 지역이나 사용자 연령과 같은 자격 조건 뿐 아니라 사용자 등급에 따른 컨텐츠 기본 이용 권한(읽기, 인쇄, 편집 등) 및 이용 횟수 제한 등과 같은 해당 컨텐츠를 이용할 수 있는 범위가 명시된다. 서비스 목록은 SP와 컨텐츠 소유권자 사이의 계약에 의해서 분류된 해당 컨텐츠가 포함될 서비스의 종류를 나타낸다.

저작권자는 자신의 만든 컨텐츠의 o_CS를 생성해서 CC에 제출하고, 해당 컨텐츠와 함께 배포자에게 o_CS를 전달된다. 배포자는 컨텐츠와 o_CS를 함께 캡슐화 시켜서 DC를 생성한다. 해당 컨텐츠를 이용하려는 사용자는 이용 규칙의 모든 항목을 만족시켜야 되며, 서비스 목록에 명시된 서비스 중 적어도 하나를 신청했어야 한다.

r_CS는 기본적으로 사용자 인증정보와 컨텐츠 사용 권한 목록으로 구성된다. 사용자 인증정보에는 CC가 부여한 사용자 id를 비롯해서 사용자의 연령, 지역, 직업 및 서비스 이용 등급 등 서비스에서 사용자를 인증하고 자격을 검증하기 위해 필요한 모든 정보가 포함된다. 컨텐츠 사용 권한 목록에는 SP가 제공하는 서비스 목록 중에서 사용자가 선택한 서비스와 해당 서비스 또는 서비스에 포함된 컨텐츠의 사용 권한(예를 들어, 1회 복사, 출력, 편집 등)으로 구성된다. 지불 시스템과 함께 운영된다면, 유료 컨텐츠 사용에 필요한 토큰(Token)과 Pay-Per-Usage(PPU) 서비스 이용 가능 여부 등이 컨텐츠 사용 권한 목록에 포함될 수 있다. 사용자 인증 정보는 사용자가 SP에 등록할 때 한번 생성된 정보를 계속 이용할 수 있으나, 컨텐츠 사용 권한 목록은 사용자가 서비스를 신청 또는 변경할 때마다 변경된다.

r_CS는 서비스 사업자가 제공하는 컨텐츠 서비스를 제공받기 위하여 사용자가 CC에 신청해서 발급 받는다. 기존의 AC 구조에서 CS가 컨텐츠를 이용하기 위해 발급 받는 것이었다면, 제안하는 구조에서는 컨텐츠 서비스를 이용하기 위하여 발급 받는다는 차이가 있다.

o_CS에 포함되어 있는 컨텐츠 id를 근거로 r_CS에 동일한 컨텐츠 id가 포함되어 있을 때만 사용자가 해당 컨텐츠를 이용할 수 있도록 서비스를 제공한다면, [7]에서 제시된 External CS 형태의 AC와 동일한 서비스를 제공할 수 있다. 뿐만 아니라, o_CS와 r_CS

에 명시된 컨텐츠 id와는 상관없이 컨텐츠 이용에 필요한 사용자 조건만 검증되면 누구나 해당 컨텐츠를 이용할 수 있도록 설정할 수도 있다. 또한 특정 사용자만 사용하도록 사용자 id를 명시할 수도 있다. 지불 시스템과 함께 시스템을 구성한다면 o_CS는 해당 컨텐츠 이용에 따른 요금 정보를 포함할 수 있다. 또한, 컨텐츠의 종류나 컨텐츠 id와 관계없이 사용자의 컨텐츠 접근 및 해당 컨텐츠의 사용에 따라 요금을 징수하는 PPU 서비스 제공 여부와 PPU 서비스에 따른 요금 정보를 함께 기록함으로써 특정 컨텐츠와 관련된 CS 없이도 사용자가 원하는 컨텐츠를(공급받는 방법에 상관없이) 이용할 수 있다.

2.2.2 운영

제안하는 AC 구조를 효과적으로 운영하기 위해서는 앞서 가정했던 것처럼 CC/SP가 기존의 CS 관리와 Usage History 관리 이외에 사용자와 컨텐츠 소유권자 사이에서 다양한 서비스를 제공할 수 있어야 한다. 또한 r_CS의 발급을 위해서 PKI의 RA/CA와 같이 사용자를 확인하고 검증하는 기능도 수행해야한다. 그리고 지불 시스템과 연동된 경우, 관련 정보의 관리 및 운영에 관한 모든 책임도 가져야한다.

제안하는 AC의 운영 순서는 다음과 같다:

① 컨텐츠 등록

- 컨텐츠 소유권자는 CC/SP에 해당 컨텐츠를 등록하고, 컨텐츠 id와 컨텐츠 서비스 분류 정보(예를 들어 종류, 성격, 시청 연령 등)를 계약에 의해서 할당받는다.
- 소유권자는 CC/SP로부터 할당받은 컨텐츠 서비스 분류 정보를 이용해서 o_CS를 작성하고, CC/SP에 작성한 o_CS를 제출한다.
- 소유권자는 컨텐츠와 o_CS를 배포자에게 전달한다.
- 컨텐츠 배포자는 소유권자로부터 전달받은 컨텐츠와 o_CS를 DC로 생성하기 위하여 캡슐화 과정을 수행한다. 컨텐츠 배포 형식에 따라 직접 사용자에게 전송하거나, 또는 외부저장소(RS)에 저장한다.
- CC/SP는 컨텐츠 소유권자가 제출한 o_CS와 기존의 다른 컨텐츠의 o_CS를 가지고 소유권자와의 계약에 따라 서비스를 구성해서 사용자에게 제시한다.

② 사용 권한 신청 :

- 컨텐츠 사용자는 CC/SP에 등록하고, 사용자 id 및 인증정보를 부여받는다. CC/SP에서 제시한 서비스 목록을 검토하고, 원하는 서비스와 해당 서비스에 포함되어 있는 컨텐츠의 사용 자격을 신청한다.
- CC/SP는 사용자 요청에 따라 r_CS를 구성하고, 사용자에게 전송한다.
- 컨텐츠 사용자는 인증기관으로부터 전송 받은 r_CS를 VM에 입력한다.

만약 유료 서비스가 제공된다면, 사용자는 토큰을 신청해서 해당 유료 서비스를 이용할 수 있다. 또한 PPU 서비스가 제공되는 경우라면, PPU 서비스 이용 허가를 신청해서 해당 서비스를 이용할 수 있다.

③ 컨텐츠 획득

- 컨텐츠 사용자는 컨텐츠 배포자나 컨텐츠 저장소(RS)로부터 컨텐츠 DC를 전송 받아 사용자 VM에 입력한다.

④ 컨텐츠 사용

- 컨텐츠 사용자의 VM은 입력된 r_CS와 컨텐츠 DC에 포함되어 있는 o_CS를 확인한다. 입력된 r_CS와 o_CS를 근거로 해서 r_CS의 소유자를 인증하고, r_CS의 소유자가 해당 컨텐츠에 접근할 수 있는지를 판단한다. 이 때, r_CS의 사용자 인증정보가 o_CS에 명시된 연령, 등급 등 컨텐츠 접근에 필요한 모든 조건이 동시에 만족 할 때만 접근을 허가한다. 그리고 해당 컨텐츠의 사용 권한을 확인해서 컨텐츠 사용을 제어한다. 예를 들어, 전자문서의 o_CS에 3급 이상의 서울지역 공무원만 읽을 수 있도록 설정되어 있다면, r_CS에 포함된 사용자 인증 정보에서 "3급 이상, 서울, 공무원" 이라는 조건이 만족되어야 하고 컨텐츠 사용 권한 목록 중에서 읽기가 설정되어 있어야만 한다.

만약 지불 시스템과 연동 중이고, 해당 컨텐츠가 (후불 서비스에서) 유료라면 이용료 지불에 충분한 토큰을 보유하고 있어야 한다. 지불 시스템과 함께 운영 중이고 해당 컨텐츠에 대하여 PPU 서비스가 제공되고 있는 경우에 VM이 o_CS와 r_CS를 확인한 결과, 사용자가 해당 컨텐츠에 대한 접근 권한을 갖고 있지 않다고 판단되면, PPU 서비스 이용 여부를 사용자에게 확인 받아 해당 서비스를 제공할 수 있다. PPU 서비스를 제공하기 위해서는 사용자가 PPU

서비스로 이용한 컨텐츠 목록을 Control Center가 (이용과 동시에 또는 이용 후에) 수집할 수 있어야한다. 이렇게 수집된 이용 정보는 사용자에게 해당 컨텐츠 이용에 따른 사용료 징수와 저작권료 지불을 위한 근거 자료로 사용될 수 있다.

2.2.3 특징 및 문제점

[표 1]은 기존에 제안된 AC 구조의 특징과 본 논문에서 제안한 AC 구조의 특징을 정리한 것이다. [7]에서 제시된 기존의 CS 형태가 '개별 컨텐츠에 대한 사용 자격'을 제어하기 위해서 사용되었다면, 제안된 AC 구조에서는 '컨텐츠 서비스에 대한 사용 자격'으로 그 범위를 확장시킴으로서 컨텐츠 저작권자와 사업자 사이의 계약에 따라 구성되는 다양한 컨텐츠 서비스를 사용자가 손쉽게 이용할 수 있다. 특히 기존의 구조에서는 제공될 수 없었던 PPU 서비스와 사용자의 특정 조건만을 확인해서 컨텐츠를 이용하게 하는 서비스가 가능하다.

또한 기존의 External AC 구조에서는 컨텐츠를 이용할 때마다 인증기관에 접속해서 필요한 CS를 다운로드 해야만 했다. 그러나 제안하는 구조에서는 서비스 신청 시에 인증기관에 접속해서 r_CS를 다운로드하면, 해당 서비스에 포함되어 있는 모든 컨텐츠를 인증기관 접속 없이 이용할 수 있다. 그러므로 사용자 측면에서 인증기관 접속 횟수를 상당히 줄일 수 있다. 또한 기존의 External AC 구조에서는 컨텐츠를 이용하기 위해서 인증기관에 접속해야 되기 때문에 네트워크에 연결된 컴퓨터나 무선 단말기 등에서만 사용이 가능했지만, 제안하는 구조는 VM이 장착된 모든 장치(예를 들어 CDP, MP3 Player, PDA 등)에 r_CS를 입력시키는 것만으로 이용이 가능하다.

그러나 이와 같은 서비스를 실제 구현하기 위해서는 r_CS를 안전하게 운영하는 방안과 유료 서비스를 위한 지불 시스템과의 연동 등이 해결되어야 한다. 특히, r_CS의 분실 및 불법 복제와 같은 문제를 해결해야 되며, 사용자 인증 문제 또한 풀어야 될 과제다. 이와 같은 문제는

- VM과 r_CS를 대응시켜서 운영하는 방안과
- 스마트카드와 같은 안전한 저장 매체를 이용하는 방안 등을 고려해 볼 수 있다. 또한
- r_CS를 저장하고 있는 DC나 r_CS 안에 사용자 비밀번호를 hash된 상태로 저장시켜 놓고, VM에서 사용자의 비밀 번호를 확인하는 방안도 부가적으로 고려해 볼 수 있다.

앞서 언급한 것처럼 본 논문의 목적이 새로운 AC 구성을 제안하는 것이므로 안전성에 관한 자세한 언급은 생략 하도록 한다.

Ⅲ. 결 론

본 논문에서 제안한 AC 구조는 기존에 제안된 구조가 컨텐츠를 이용할 때마다 CS를 획득해야 하거나, VM을 공통적으로 이용할 수 없다는 단점을 감안해서 컨텐츠 소유권자에 의해서 작성한 o_CS와 컨텐츠 사용자를 위한 r_CS를 이용하여 사용자가 필요에 따라 미리 원하는 컨텐츠들의 사용 권한들을 확보해 둘 수 있도록 설계되었으며, PPU와 같은 서비스가 가능하도록 구성하였다. 이를 위해 컨텐츠 기반의 제어가 아닌 컨텐츠 서비스 기반의 제어를 선택했다. 특히, 제안한 AC 구조에서 VM은 o_CS와 r_CS를 검증하고, 그 결과에 따라 컨텐츠를 사용할 수 있도록 제공하는 역할만을 수행하기 때문에 특정 사용

〔표 1〕 AC 특징 비교

	특 징	NC	FC	EC	XC	TC
S1	배포자는 배포한 컨텐츠의 접근 및 사용을 제어할 수 있다.		Y	Y	Y	Y
S2	컨텐츠가 배포된 이후에 사용자의 접근권한을 변경할 수 있다.				Y	Y
S3	컨텐츠의 재배포는 제어될 수 있다.		Y	Y	Y	Y
F1	컨텐츠를 이용하기 위해서는 특정 응용프로그램이 필요하다.		Y	Y	Y	Y
F2	컨텐츠 재배포 절차를 통해서 배포된 컨텐츠는 다른 사용자가 이용할 수 있다.				Y	Y
F3	사용자는 여러 단말기에서 컨텐츠를 이용할 수 있다.	Y	Y	Y	O	O
F4	네트워크 접속 없이 이용이 가능하다. 즉, 오프라인 단말기에 응용할 수 있다.	Y				Y
F5	컨텐츠 예약 서비스가 가능하다.					Y
F6	Pay-Per-Usage 서비스가 가능하다.					Y

자나 컨텐츠에 관계없이 사용될 수 있다. 그러므로, r_CS를 스마트카드와 같은 안전한 저장 장치와 함께 운영한다면 쉽게 사용자 플랫폼을 변경해서 사용할 수 있으며, 사용자 플랫폼이 CDP와 같은 오프라인 장치에도 응용이 가능하다. 또한 제안된 AC 구조는 DRM과 같은 컨텐츠 유료 서비스 뿐 아니라 디지털 문서 보관소와 같은 PFT 서비스에도 적용이 가능하다.

앞서 언급한 것처럼 본 논문의 목적에 따라 제안된 구조는 운영의 안전성 측면을 충분히 고려하지 않았다. 그러므로 실제 시스템 설계 및 운영에 있어서 안전성 측면을 충분히 고려해야 되고, 서비스의 대중성을 위해서는 다양한 서비스 종류의 개발과 이를 지원할 수 있는 효과적인 Control Set의 설계가 계속 연구되어야 한다.

참 고 문 헌

[1] EBU Project Group B/CA, "Functional model of conditional access system", *EBU Technical Review*, pp. 64~77, winter 1995.

[2] Francoise Coutrot, Vincent Michon, "A Single Conditional Access System for Satellite-Cable and Terrestrial TV", *IEEE Trans. on Consumer Electronic*, Vol. 35, No. 3, pp. 464~468, Aug. 1989.

[3] Didier Angebaud, JeanLuc Giachetti, "Conditional Access Mechanisms for All-Digital Broadcast Signals", *IEEE Trans. on Consumer Electronic*, Vol. 38, No. 3, pp. 188~194, Aug. 1992.

[4] 이창열, "DRM 기술", *정보보호학회지*, 제12권, 제1호, pp. 1~10, 2002년 2월.

[5] 전종민, 최영철, 박상준, 박성준, "DRM 기술 및 제품 동향 분석", *정보보호학회지*, 제 11권, 제5호, pp. 26~34. 2001년 10월.

[6] Renato Iannella, "Digital Rights Management Architectures", *D-Lib Magazine*, Vol. 7, No. 6, June 2001.

[7] Park JaeHong, Ravi Sandhu., James Schifalacqua., "Security Architectures for Controlled Digital Information Dissemination", *Proceedings of the 16th Annual Computer Security Application Conference*, 2000.

〈著者紹介〉

김 대 엽 (Dae-Youb Kim) 정회원
1994년 2월 : 고려대학교 수학과 졸업
1996년 8월 : 고려대학교 수학과 석사(대수학 전공)
2000년 2월 : 고려대학교 수학과 박사(대수학 전공)
1997년 8월~2001년 3월 : (주)텔리맨, 위성통신 연구소, CAS팀 선임연구원
2001년 4월~2002년 7월 : 삼성 시큐아이닷컴(주) 정보보호 연구소 PKI실 차장
2002년 9월~현재 : 삼성 종합기술원, i-Networking Lab. 전문연구원
<관심분야> CAS, DRM, PKI/WPKI, Smart Card, 응용 보안프로토콜

주 학 수 (Hak-Soo Ju)
1997년 8월 : 고려대학교 수학과 졸업
1999년 8월 : 고려대학교 수학과 이학석사(대수학 전공)
2001년 8월 : 고려대학교 수학과 박사과정 수료
2001년 9월~현재 : 한국정보보호진흥원 연구원
<관심분야 > ECC, 워터마킹, PKI