논문 2009-46CI-2-2

휴대용 보안 저장매체 기반 방송프로그램 사적이용 인증 기법

(Personal-usage Authentication of Broadcast Programs Using a Secure Portable Storage)

이 주 영*, 추 현 곤*, 남 제 호*

(Jooyoung Lee, Hyon-Gon Choo, and Jeho Nam)

요 약

본 논문에서는 휴대용 보안 저장매체를 이용한 방송프로그램의 사적이용 인증을 통해, 도메인에 등록된 휴대용 사적이용 인증기기를 보유한 사용자가 물리적인 장소에 구애 받지 않고 자신이 녹화한 방송프로그램을 자유롭게 사용할 수 있도록 함으로써 사용자의 사적이용을 보장할 수 있는 방법을 제안한다. 본 논문에서 제안하는 사적이용 인증과정은 휴대용 사적이용 인증기기, 휴대용 사적이용 인증기기 접근제어 모듈, 휴대용 사적이용 인증기기 연동 재생 툴에 의해 이루어진다. 휴대용 사적이용 인증기기는 도메인 인증정보를 보호된 상태로 안전하게 저장할 수 있는 저장매체 역할을 수행하며, 휴대용 사적이용 인증기기 접근제어 모듈은 휴대용 사적이용 인증기기에 저장된 도메인 인증정보와 방송프로그램의 인증정보를 이용하여 방송프로그램 재생 정보를 추출하는 역할을 수행한다. 휴대용 사적이용 인증기기 연동 재생 툴은 휴대용 사적이용 인증기기 접근제어 모듈을 통해 획득한 방송프로그램 재생 정보를 이용하여 사용자의 명령에 따라 보호된 방송프로그램을 복호화 재생하는 기능을 제공한다. 본 논문에서는 제안 모델의 구성과 동작 절차를 기술하고 구현을 통해 제안한 인증방법에 대한 유효성 검증을 수행한다.

Abstract

In this paper, we propose a novel method for authenticating a user's personal-usage using a secure portable storage, so that the user carrying the secure portable storage is able to consume his/her own broadcast programs freely, regardless of the location of the devices. The proposed authentication process is performed by a portable personal-usage authentication device, an access-control module for the portable personal-usage authentication device, and a player integrating the access control module. The portable personal-usage authentication device plays a role of secure storage in which domain authentication information is securely stored, while the access-control module is in charge of accessing the authentication information and, consequently, acquiring a decryption key. The player decrypts the broadcast programs in real time and processes the decrypted media streams. In this paper, we describe the structure and procedure of the proposed model, and verify its feasibility by implementation.

Keywords : Broadcast Programs, Authentication, DRM, Personal-usage

Ⅰ. 서 론

디지털 콘텐츠 시장이 확대됨에 따라 불법 디지털 콘텐츠 사용에 따른 피해도 늘어나고 있으며, 이는 복사가 쉽고 빠르며, 복사본이 원본과 동일한 품질을 갖는 디지털 콘텐츠의 특성에 기인한다. 이에 디지털 콘텐츠의 불법 복제 및 사용을 기술적으로 막고자 하는 DRM(Digital Rights Management)에 대한 연구가 진행되고 있다. 초기 DRM은 단일 디바이스 단위의 불법 복제 방지 기술로 이루어졌으나, 이는 사용자가 보유한 여러 단말 간의 콘텐츠 이동을 제한함으로써 사적이용 침해에 대한 문제점을 발생시켰고, 이에 사용자가 보유한 복수의 단말을 하나의 그룹으로 묶어 자유로운 복사

* 정회원, 한국전자통신연구원 방통미디어연구부
(Broadcasting & Telecommunications Media Research Department, ETRI)

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S-003-03, 지상파DTV 방송프로그램 보호 기술 개발]

접수일자: 2009년2월20일, 수정완료일: 2009년3월6일

와 공유가 가능토록 하는 도메인(Domain) 기술에 대한 연구가 진행되고 있다.

그러나 현재의 등록 기반 도메인 기술은 사적이용의 기술적 범위를 도메인에 등록(가입)한 기기들로 한정하며 이는 기기 등록이 불가능한 외부 기기의 경우 비록 사용자의 개인적인 사용일지라도 콘텐츠 복사·재생을 지원하지 않는 문제점을 발생시킨다. 즉 단순 등록 기반의 도메인 기술은 엄밀한 의미의 사적이용보다 훨씬 제약적인 콘텐츠 사용 범위를 만들게 되며 이는 사용자의 이용 편의성을 크게 저해한다. 따라서 콘텐츠 이용 주체에 대한 인증을 통한 사적이용 지원 기술의 확장이 필요하다.

사용자 인증 방식은 크게 사용자가 알고 있는 정보("What you know"), 사용자가 보유하고 있는 사물이나 장치("What you have"), 사용자 고유의 특징("Who you are") 등을 이용하는 방식으로 구성되나, ID/PW 등 사용자가 알고 있는 정보는 악의적인 목적으로 콘텐츠와 함께 배포가 가능하고, 지문, 홍채 등 사용자 고유의 정보는 기술의 구현 부담이 지나치게 큰 경향이 있다. 따라서 사용자가 보유하는 장치를 기반으로 사용자 인증을 지원하는 방법이 가장 적합하다. 본 논문에서는 사용자가 보유한 장치 기반의 사적이용 인증 방법을 제안하며, 특히 외부 네트워크 연결을 보장할 수 없는 방송 환경의 방송프로그램에 대한 사적이용 인증 방법을 대상으로 한다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 사적이용 인증을 위한 연구 배경을 기술하고 문제를 정의한다. Ⅲ장에서는 제안 기술의 구성 및 제안 동작 절차를 기술하고 Ⅳ장에서는 구현 및 검증을 수행하며 Ⅴ장에서 결론을 맺는다.

Ⅱ. 연구 배경

1. 관련 연구

도메인 기술은 도메인 외부의 관리 서버가 도메인 구성원 권한을 발급하는 구조와, 도메인을 구성하는 일부 기기가 도메인 구성원 권한을 발급하는 구조로 나눌 수 있다. 사적이용권은 특정 서비스 제공자와는 독립적으로 항상 보장되어야 하는 사용자의 권리이므로 외부 인증기관 없이 사용자의 기기를 통해 직접 도메인 구성하는 후자가 사적이용권을 보장하기 위한 목적에 더 적합하다. 또한 무료 보편적인 지상파 방송망과 같이 외부 서버로의 연결에 대한 보장을 할 수 없는 경우, 사용자가 보유한 기기 간의 자체적인 사적이용범위를 구성해야 한다. 따라서 본 논문에서는 외부 인증기관 없이 자체적으로 사적이용을 보장하는 기술에 대해서만 고려하며, 기 연구된 기술로 DVB-CPCM[1], Dubbing10[2], 지상파DTV 사적이용범위 지원 기술[3] 등이 있다.

가. DVB-CPCM

유럽의 디지털 방송 기술은 DVB 표준을 중심으로 적용되고 있으며, DVB-CPCM[1]은 방송프로그램의 저작권 보호를 위한 단말 기기의 기술 표준이다. DVB-CPCM은 사용자 기기 간의 방송프로그램 복사를 위해 ADM(Authorized Domain Management) 기술을 정의하고 AD(Authorized Domain)에 등록된 기기 간에 방송프로그램을 자유롭게 복사할 수 있도록 하였다. 그러나 DVB-CPCM의 ADM은 사적이용범위의 기술적 지원이 아닌 범용 목적의 사용자 디바이스 그룹 관리를 목적으로 하며, 다음과 같은 이유로 사적이용을 위한 기술적 지원이 어렵다.

DVB-CPCM ADM 기술은 사용자 내지는 가족구성원이 보유한 기기 간의 방송프로그램 공유 및 이용을 지원하지만 이용 주체에 대해서 고려하지 않으므로 사용자가 녹화를 통해 보유한 방송프로그램을 외부 기기(등록이 불가능하거나 등록할 경우 사적이용범위를 넘어서는 기기, 예: 출장지 PC방의 PC)에서 재생하기 어렵다. DVB-CPCM ADM은 리모트 환경의 도메인을 위해 별장(Second Home) 도메인 개념을 도입하고 있지만, 별장 도메인은 네트워크를 통해 연결되는 외부 기기들의 그룹이기 때문에 제 3의 외부 인증기관이 없을 경우 악용될 위험이 높다. 또한 PC방과 같이 공공장소의 기기는 불특정 다수의 사용자가 접근할 수 있기 때문에 별장 도메인 개념을 적용하기에는 어려움이 있다. 또한 DVB-CPCM ADM은 도메인 구성에 대한 지나친 제어 기능을 수행한다. DVB-CPCM ADM은 등록가능기기 수, 로컬 등록가능기기 수, 리모트 등록가능기기 수, Domain Controller(DC) 분할 가능 횟수 등 다양한 변수를 이용하여 도메인 등록 및 방송프로그램 이용을 제어한다. 그러나 이같은 변수를 통한 사용자의 도메인에 대한 통제(Governance)는 특정 서비스 제공자에 의해 사용자의 사적이용을 제한하는 결과를 가져올 수 있다. 또한 DVB-CPCM ADM 기술은 사용자의 도메인에 대한 이해를 요구한다. DVB-CPCM ADM은 다양한 도메인 구조를 유지하기 위해

관리기기(DC:Domain Controller)의 분할(split), 병합(merge), 재조정(rebalancing) 등 다양한 프로토콜을 이용하며, 분할된도메인 관리기기는 등록 가능한 기기의 수를 나누어 관리한다. 그러나 관련 프로토콜 수행을 위한 기기 간 연결이 적시에 이루어지지 않을 경우, 사용자의 정당한 이용을 제약하는 원인이 될 수 있으므로 사용자는 도메인의 현재 상태를 인지해야 하는 부담이 있다.

나. Dubbing10

일본에서는 디지털 방송프로그램의 저작권을 보호하기 위해 "copy once" 방식을 채택하여 사용해왔으나, 이는 방송프로그램의 복사 횟수를 1회로 제한하기 때문에 사용자의 사적이용을 크게 제약하는 문제점을 발생시켜 소비자 단체의 큰 반발을 유발해왔다. 이에 일본 총무성 정보통신심의회에서 디지털 방송의 사적이용에 관한 완화된 운영 규칙을 제시하였고, 전자정보기술산업협회 (JEITA)는 이를 "Dubbing10"으로 명명하였다. Dubbing10은 일본 디지털 TV 방송의 저작권 보호를 위한 방법으로 2008년 7월 4일부터 일본의 지상파 디지털 방송, 위성 디지털 방송을 대상으로 운용이 시작되었다.

Dubbing10은 사용자가 녹화한 방송프로그램을 10회 복사(9회 복사 후 10회 째 복사 시 원본 삭제)할 수 있도록 허용한다. 복사는 DVD, 블루레이 등의 분리형 매체 또는 연결된 기기를 대상으로 가능하다. Dubbing10은 기존의 "copy once" 방식에 비해 방송프로그램 사용 제약을 크게 완화하였으나, 여전히 횟수를 기반으로 하는 단순한 제어 방식이며 복사된 방송프로그램의 개인적인 추가 재배포가 불가능한 점은 사용자의 사적이용을 크게 제약한다. 또한 Dubbing10은 모든 경우에 10회 복사가 가능한 것이 아니라, 방송프로그램에 따라 1회 복사 또는 복사 불가 신호를 송출함으로써 서비스 사업자에 의해 사용자의 사적이용이 제한되는 경우도 발생할 수 있다.

다. 지상파DTV 사적이용범위 지원 기술

국내에서는 지상파 디지털 방송프로그램을 위한 기술적 보호 조치를 마련하기 위해 ETRI와 방송 4사(KBS, MBC, SBS, EBS) 및 여러 산업체를 중심으로 차세대방송표준포럼 방송콘텐츠보호관리분과위원회[7]를 통한 기술 표준 활동이 이루어지고 있다. 2008년 TTA의 방송프로그램 보호 신호(PPI: Program Protection Information)의 표준 제정을 완료하였고, 2009년에는 단말의 방송프로그램 사적이용 지원을 위한 기술 개발을 수행하고 있으며 그 일환으로 [3]의 사적이용 지원 기술을 정의하고 있다. [3]에서는 도메인 등록 방식과 기기 인증 방식의 장점을 혼합한 방송프로그램 사적이용 관리를 위한 기술 지원 방식을 정의한다. 도메인 등록 방식에 의한 방송프로그램 공유 방식의 특징은 도메인 등록 기기 간의 복사 경로에 상관없이 복사 및 재생이 가능하고, 사용자의 다양한 기기 구성에 유연하게 대응 가능하다는 장점이 있다. 또한 [3]의 방송프로그램 사적이용 지원 모델은 도메인 등록이 불필요한 연결 기기의 일회성 이용을 위해 기기 인증 기능을 제공한다.

2. 문제 정의

상기 언급한 바와 같이 각국에서는 방송프로그램 사적이용 지원을 위한 기술적 보호조치를 마련하고 있으나, 현재는 방송프로그램 이용 기기를 중심으로 사적이용 범위의 기준이 정의되어 있으며, 이는 기기에 대한 등록이나 인증이 불가능한 외부 기기에서의 정당한 방송프로그램 이용에 제약을 줄 수 있다. 따라서 외부 기기에서 방송프로그램 이용 주체에 대한 인증을 통해 정당한 방송프로그램 이용을 지원할 수 있는 방법이 필요하며, 이는 서비스 제공자와는 독립적으로 사용자의 사적이용권을 보장하기 위해 외부 인증기관의 관여 없이 이루어져야 한다. 본 논문에서는 사용자가 보유하는 장치를 기반으로 사용자의 정당한 사용권한을 인증하는 방법을 제안한다.

Ⅲ. 제안 기술

1. 휴대용 사적이용 인증기기 이용 시나리오

본 논문에서는 사적이용 인증을 지원하는 휴대용 보안 저장매체(예: 보안 USB)를 휴대용 사적이용 인증 기기로 정의한다. 휴대용 사적이용 인증 기기를 통한 도메인 외부의 사적이용 인증 시나리오는 다음의 세 단계를 거치며 이는 그림 1에 나타나 있다. 그림 1에서 사용자는 자신의 사적이용을 관리하는 도메인 관리기기에 휴대용 사적이용 인증 기기를 연결하고 해당 기기를 도메인 관리기기가 관리하고 있는 도메인에 등록한 후, 사용자는 자신의 도메인에 등록되지 않은 외부 기기에서 자신의 방송프로그램을 이용하기 위해 자신의 도메

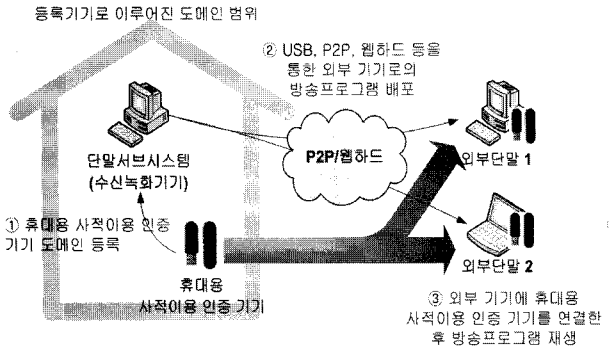


그림 1. 사적이용 인증 시나리오
Fig. 1. Scenario of personal-usage authentication.

인에 등록된 휴대용 사적이용 인증 기기를 연결한다. 휴대용 사적이용 인증 기기가 연결된 기기는 휴대용 사적이용 인증 기기에 저장된 인증정보와 방송프로그램 패키지*에 저장된 인증정보를 이용한 인증 과정을 거쳐 재생 정보를 획득하고 이를 이용하여 방송프로그램을 복호화 재생한다.

2. 사적이용 인증 구성

휴대용 사적이용 인증 기기 기반 사적이용 인증 모델은 도메인 외부의 기기가 임시적으로 도메인에 속한 방송프로그램을 재생할 수 있도록 하는 기능을 제공한다. 이를 지원하기 위한 구성요소는 휴대용 사적이용 인증 기기, 휴대용 사적이용 인증 기기 접근제어 모듈, 휴대용 사적이용 인증 연동 재생 툴로 이루어지며 다음은 각각의 기본적인 기능을 기술한 것이다.

가. 휴대용 사적이용 인증 기기

휴대용 사적이용 인증 기기는 사용자가 실제로 휴대하는 보안 USB 등의 기기이며 도메인 등록 기기가 보유하는 도메인 인증정보를 보호된 상태로 저장하는 기능을 제공한다. 휴대용 사적이용 인증 기기의 구조는 그림 2와 같다. 휴대용 사적이용 인증기기의 데이터 저장 영역은 보호 저장 영역과 일반 저장 영역으로 구분된다. 보호 저장 영역은 보안성이 필요한 데이터를 저장하는 영역이며 일반적인 파일 시스템 구조와는 다른 고유 저장 방식을 이용하여 운영체제를 통한 사용자의 접근을 방지한다. 애플리케이션이 보호 저장 영역에 접근하기 위해서는 휴대용 사적이용 인증 기기 접근제어

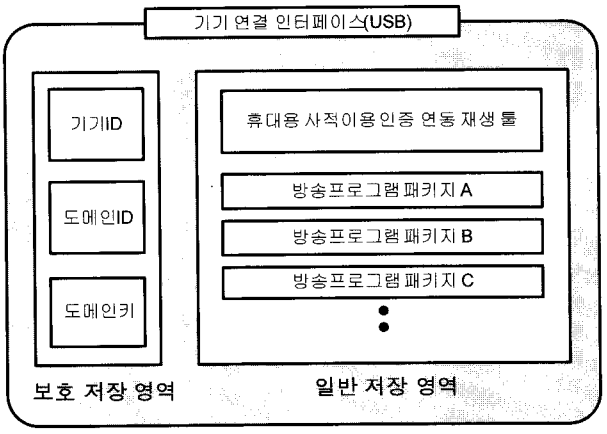


그림 2. 휴대용 사적이용 인증기기 구조
Fig. 2. Structure of a portable personal-usage authentication device.

모듈을 통해서만 가능하다. 보호 저장 영역은 해당 기기의 고유 ID와 휴대용 사적이용 인증 기기가 등록된 도메인ID, 그리고 도메인 등록 권한을 나타내는 도메인 키를 포함한다. 상기 데이터는 복사가 불가능하며, 강제적인 복사가 이루어지더라도 기기 고유의 키로 암호화 되어있기 때문에 해석이 불가능하다. 도메인ID와 도메인 키 정보의 세부 내용은 표 1과 같다. 일반 저장 영역은 휴대용 사적이용 인증 기기 내에 일반적인 파일 시스템을 통해 접근이 가능한 영역이다. 일반 저장 영역에는 휴대용 사적이용 인증 연동 재생 툴의 실행파일이나 방송프로그램, 그 밖에 다양한 사용자의 데이터를 저장할 수 있다.

표 1. 휴대용 사적이용 인증기기 저장 정보
Table 1. Data types stored in the portable personal-usage authentication device.

관리정보	길이(bit)	정보 수	의미
기기 ID	128	1	휴대용 사적이용 인증 기기의 고유 ID
도메인ID	128	1	휴대용 사적이용 인증기기가 등록된 도메인ID
도메인키	128	1	도메인 등록 권한 키

나. 휴대용 사적이용 인증 연동 재생 툴

휴대용 사적이용 인증 연동 재생 툴은 휴대용 사적이용 인증 기기가 연결되어 있는 기기에서 휴대용 사적이용 인증 기기 접근제어 모듈을 통해 방송프로그램의 재생 권한을 획득하여 방송프로그램을 재생하거나 휴대용 사적이용 인증 기기를 특정 도메인에 등록하는 기능을

* 방송프로그램 패키지는 암호화된 방송프로그램, 사적이용 인증정보, 방송프로그램 메타데이터 등이 포함된 파일 형태의 패키지를 의미한다.

제공한다. 그림 3은 휴대용 사적이용 인증 연동 재생 툴의 구조를 나타낸다. 그림 3에서 재생 툴 제어모듈의 사용자 입력에 따라 재생 툴의 각 모듈을 제어하고, 명령 처리결과를 사용자에게 반환하는 역할을 수행한다. 패키저 모듈은 저장된 방송프로그램 패키지로부터 사적이용 인증 정보와 암호화된 방송프로그램 등을 추출하는 기능을 제공한다. 휴대용 사적이용 인증기기 접근제어 모듈은 방송프로그램 패키지의 사적이용 인증정보와 휴대용 사적이용 인증기기에 저장된 도메인 키 정보를 이용하여 방송프로그램의 복호화 재생 정보를 추출하는 기능을 제공한다.

다. 휴대용 사적이용 인증 기기 접근제어 모듈

휴대용 사적이용 인증 기기 접근제어 모듈은 휴대용 사적이용 인증 기기에 도메인 인증 정보를 저장하고, 저장된 정보를 이용하여 방송프로그램의 재생 정보를 획득하는 기능을 제공한다. 휴대용 사적이용 인증 기기 접근제어 모듈은 휴대용 사적이용 인증 연동 재생 툴에 의해 호출되며, 다음과 같은 기능을 제공하는 API를 통해 재생 툴과의 독립성을 유지한다.

(1) 휴대용 사적이용 인증 기기 인식 기능

휴대용 사적이용 인증 기기 접근제어 모듈은 현재 연결된 휴대용 사적이용 인증기기를 인식하고, 해당 기기 정보와 해당 기기가 등록되어 있는 도메인 정보(도메인 ID 등)에 대한 리스트를 획득하는 기능을 제공한다.

(2) 휴대용 사적이용 인증 기기 등록 및 해지 기능

휴대용 사적이용 인증 기기 접근제어 모듈은 휴대용 사적이용 기기에 도메인키 및 도메인ID를 보호된 형태로 저장하여 해당 기기를 도메인에 등록하거나, 저장된 도메인키와 도메인ID 등을 삭제하여 해당 기기를 도메인으로부터 탈퇴시키는 기능을 제공한다.

(3) 재생정보 추출 기능

패키지키와 패키지키 정보를 수신하고 휴대용 사적이용 인증 기기에 저장된 도메인 인증 정보를 이용하여 해당 패키지키로부터 재생 정보(CW: Control Word)를 추출하는 기능을 제공한다. 재생 툴은 휴대용 사적이용 인증 기기 접근제어 모듈을 통해 특정 방송프로그램에 대한 재생 정보를 획득할 수 있지만, 도메인키는 도메인 인증 유닛, 휴대용 사적이용 인증 기기 제어 유닛, 보안 영역 접근 유닛을 통해 휴대용 사적이용 인증기기 접근제어 모듈의 내부에서 처리되므로 도메인키가 유출되어 악용될 위험을 방지할 수 있다.

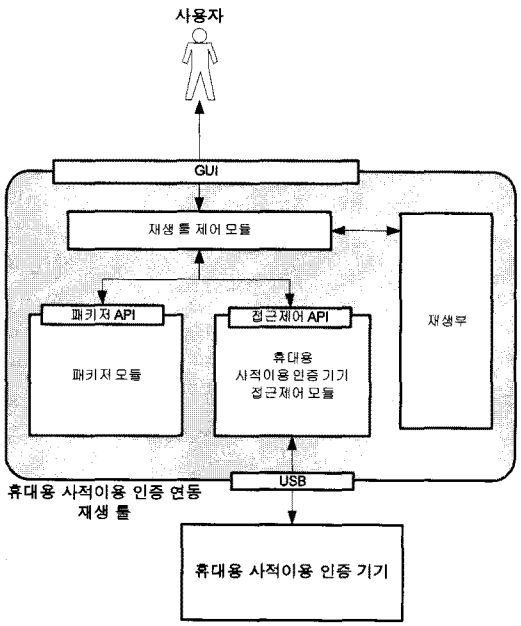


그림 3. 휴대용 사적이용 인증 연동 재생 툴 구조
Fig. 3. Structure of a player supporting personal usage authentication.

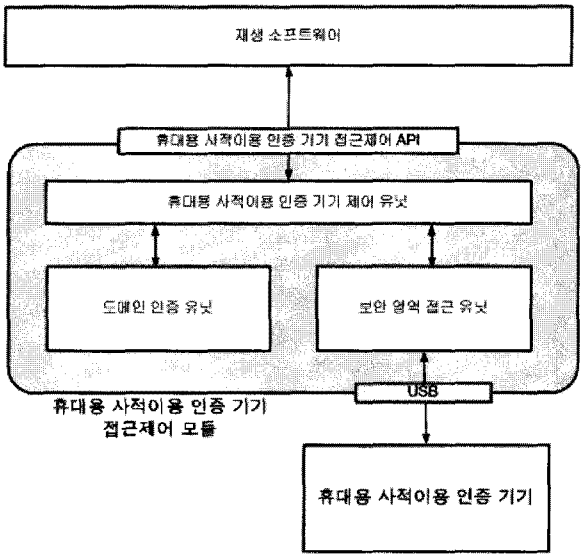


그림 4. 휴대용 사적이용 인증기기 접근제어 모듈
Fig. 4. Structure of an access-control module for the portable personal-usage authentication device.

3. 사적이용 인증 절차

도메인에 등록되지 않은 기기에서 사용자가 휴대용 사적이용 인증기기를 이용하여 방송프로그램을 재생하는 경우 휴대용 사적이용 인증 연동 재생 툴, 휴대용 사적이용 인증기기 접근제어 모듈, 휴대용 사적이용 인증기기는 그림 5와 같은 사적이용 인증 과정을 수행한다.

그림 5에서 사용자가 특정 방송프로그램에 대한 재생 명령을 내릴 경우, 휴대용 사적이용 인증기기 연동 재생 툴은 방송프로그램 패키저 모듈을 이용하여 방송프로그램 패키지로부터 사적이용 인증정보를 추출하고 이를 휴대용 사적이용 인증기기 접근제어 모듈로 전달한다. 사적이용 인증정보는 도메인키로 암호화된 방송프로그램 복호화키(CW: Control Word), 방송프로그램이 속한 도메인ID, 암복호화 알고리즘 정보 등으로 이루어지며, 휴대용 사적이용 인증기기 접근제어 모듈은 방송프로그램의 사적이용 인증 정보 내에 명시된 도메인 ID에 해당하는 휴대용 사적이용인증기기가 연결되어 있는지를 확인한다. 방송프로그램 재생을 위한 휴대용 사적이용 인증기기가 연결되어 있는 경우, 휴대용 사적이용 인증기기 접근제어 모듈은 방송프로그램 복호화키(CW) 추출 과정을 통해 방송프로그램 재생에 필요한 재생 정보(방송프로그램 복호화키(CW), 방송프로그램 암복호화 알고리즘 정보)를 획득하고 이를 재생 툴로 전달하여 방송프로그램을 복호화 재생할 수 있도록

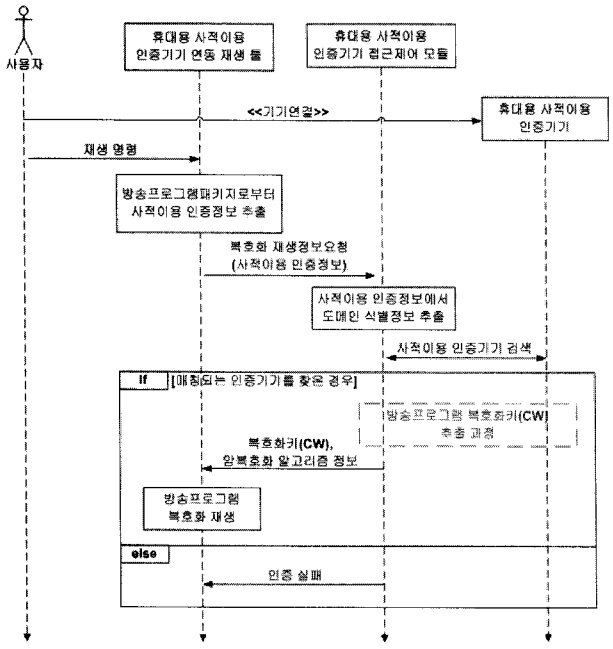


그림 5. 사적이용 인증 과정
Fig. 5. Sequence of personal-usage authentication.

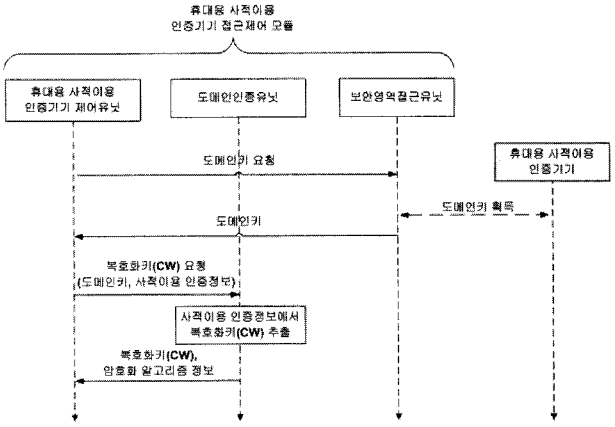


그림 6. 복호화키(CW) 추출 과정
Fig. 6. Sequence of Control Word(CW) extraction.

한다.

휴대용 사적이용 인증기기 접근제어 모듈의 복호화키(CW) 추출 과정은 그림 6과 같다. 그림 6에서 휴대용 사적이용 인증기기 제어유닛은 보안영역접근유닛으로 도메인ID에 해당하는 휴대용 사적이용 인증기기에 저장된 도메인키를 요청하고, 보안영역접근유닛은 비공개 API를 통해 휴대용 사적이용 인증기기로부터 도메인키를 획득하여 이를 휴대용 사적이용 인증기기 제어유닛으로 전달한다. 휴대용 사적이용 인증기기는 획득한 도메인키와 사적이용 인증정보를 도메인 인증유닛으로 전달하여 방송프로그램 복호화 정보를 요청한다. 도메인 인증 유닛은 사적이용 인증정보에서 도메인키로 암호화된 방송프로그램 복호화키(CW)를 추출하고 이를 입력받은 도메인키로 복호화하여 방송프로그램 복호화키(CW)를 획득한다. 도메인 인증유닛은 획득한 복호화키(CW)와 사적이용 인증정보에서 추출한 방송프로그램의 암복호화 알고리즘 정보를 휴대용 사적이용 인증기기 제어유닛을 통해 휴대용 사적이용 인증기기 연동 재생 툴로 전달하여 방송프로그램을 재생할 수 있도록 한다.

Ⅳ. 구현 및 검증

본 논문에서는 제안한 사적이용 인증 방식에 대한 구현 및 검증을 실시하기 위해 하드웨어 기반의 AES 암호화를 수행하는 Skymedi SK6203 칩셋이 장착된 16GB MLC USB 메모리를 이용하여 휴대용 사적이용 인증기기를 제작하였다. 해당 기기의 보안 저장 영역에 암호화되어 저장된 도메인ID, 도메인키, 장치ID 등의

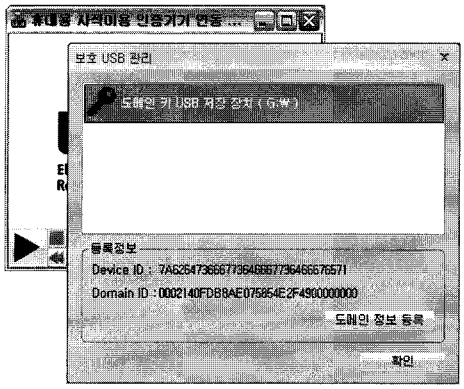
표 2. 휴대용 사적이용 인증기기 구현 및 실험 환경
Table 2. Development and test environment of a portable personal-usage authentication device.

구현 환경	
항목	환경
IDE	Microsoft Visual Studio 2008
보안 저장매체	16 GB MLC USB
보안 저장매체제어 칩셋	Skymedi SK6203
보안 저장매체 암호화 알고리즘	AES-128
도메인키 암호화 알고리즘	AES-128
방송프로그램 암호화 알고리즘	AES-128 Partial Encryption
실험 환경	
항목	환경
CPU	Intel Core2Duo 2.40GHz
RAM	2GB
OS	Windows XP Professional
방송프로그램 스트림	MPEG-2 Transport Stream
도메인 등록 가능최대 인증기기 수	5개

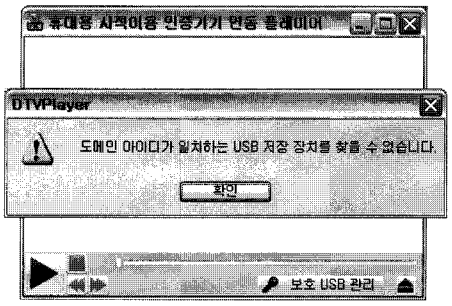
정보는 OS 레벨의 파일시스템을 통해 접근이 불가능함을 확인하였다. 더불어 휴대용 사적이용 인증기기 접근 제어 모듈과 휴대용 사적이용 인증 연동 재생 툴을 구현하고, 방송프로그램의 도메인에 해당하는 휴대용 사적이용 인증기기가 연결된 상태에서만 재생이 가능함을 확인하였다. 표 2는 본 기술의 구현 및 실험 환경을 나타낸 것이다.

그림 7은 구현한 방송프로그램 사적이용 인증 연동 재생 툴의 사용자 인터페이스이다. 그림 7-(a)는 현재 기기에 연결된 방송프로그램 사적이용 인증 기기 리스트를 나열한 화면이며, 그림 7-(b)는 방송프로그램이 속한 도메인에 해당하는 휴대용 사적이용 인증기기가 연결되어 있지 않은 경우의 인증 실패를 나타내는 화면이다. 그림 7-(C)는 적합한 휴대용 사적이용 인증기기가 연결된 경우 사적이용 인증과정을 통해 방송프로그램을 복호화하여 재생하는 화면이다.

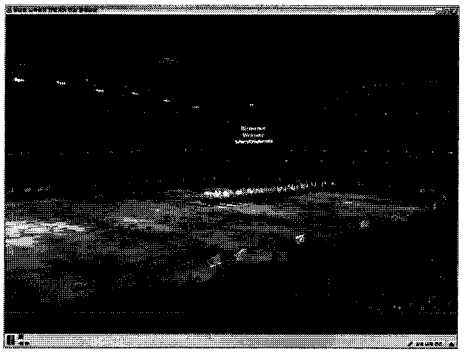
표 3은 [4]에서 정의한 사적이용 시나리오 중 방송프로그램이 녹화된 장소와 물리적으로 분리된 외부의 기기에서 해당 방송프로그램을 이용하는 사적이용 시나리오를 나열하고 각 시나리오에 대해 본 논문의 제안 기술, DVB-CPCM ADM, Dubbing10의 기술적 지원 가



(a) 방송프로그램 사적이용 인증 기기 리스트



(b) 사적이용 인증 실패 화면



(c) 사적이용 인증 후 복호화 재생화면

그림 7. 사적이용 인증 연동 재생 툴의 사용자 인터페이스
Fig. 7. User interface of a player supporting personal usage authentication.

능 여부를 나타낸 것이다. 시나리오 1, 2는 도메인 외부의 재생 시도이지만 개인적인 장소에서의 이용이며, 시나리오 3~6은 공공장소에 위치한 외부 기기에서의 재생 시도이다. 시나리오 7은 도메인 외부에서 복사해 온 방송프로그램에 대한 이용 시나리오이다.

제안 기술은 시나리오 1~6과 같이 휴대용 사적이용 인증기기를 소지하는 경우 이용 위치에 상관없이 방송프로그램의 다양한 사적이용을 지원한다. 또한 휴대용 사적이용 인증기기가 분리된 후에는 타인의 사용을 방

표 3. 사적이용 시나리오 및 접근방식 비교
Table 3. Personal-usage scenarios and comparison of approaches.

번호	사적이용 시나리오	지원 여부					
		제안 기술		DVB-CPCM ADM		Dubbing-10	
		지원 여부	위험도	지원 여부	위험도	지원 여부	위험도
1	집에서 녹화한 TV드라마를 내 USB에 복사한 후 회사에서 회사 PC로 계속 시청한다.	지원	낮음	조건부 지원[2]	낮음	조건부 지원[3]	낮음
2	집에서 TV드라마를 녹화하여 USB 포트로 외장HDD에 복사한 후, 부모님 댁의 TV/PC를 이용하여 시청한다.	지원	낮음	조건부 지원[2]	낮음	조건부 지원[3]	낮음
3	집에서 TV드라마를 녹화하여 USB포트로 외장HDD에 복사한 후, 휴양지 호텔의 TV/PC를 이용하여 시청한다. (단, 복사된 TV드라마는 내가 사용한 이후에 볼 수 없다.)	지원	낮음	조건부 지원[2]	높음	조건부 지원[3]	낮음
4	집에서 TV드라마를 녹화하여 인터넷을 통하여 웹하드에 업로드하고 휴양지 호텔에서 해당 파일을 다운로드한 후, 호텔의 TV/PC를 이용하여 시청한다. (단, 복사된 TV드라마는 내가 사용한 이후에 볼 수 없다.)	지원	낮음	조건부 지원[2]	높음	조건부 지원[3]	낮음
5	웹하드에 개인적으로 업로드한 TV드라마 녹화본을 동네 PC 방에서 시청한다. (단, 복사된 TV드라마는 내가 사용한 이후에 볼 수 없다.)	지원	낮음	조건부 지원[2]	높음	조건부 지원[3]	낮음
6	저장매체에 복사된 TV드라마를 동네 PC 방에서 시청한다. (단, 복사된 TV드라마는 내가 사용한 이후에 볼 수 없다.)	지원	낮음	조건부 지원[2]	높음	조건부 지원[3]	낮음
7	처갓집의 셋탑에 녹화저장된 TV드라마를 저장매체에 복사한 후 집에서 시청한다.	조건부 지원[1]	낮음	조건부 지원[2]	낮음	조건부 지원[3]	낮음

1) 휴대용 사적이용 인증기기의 대여/양도 후 이용 가능
2) 리모트 도메인 생성을 위해 외부 인증기관의 관여 없이 이용 주체에 대한 인증기능이 제공될 경우에 한해 가능
3) Dubbing-10은 시나리오의에 명시된 이동식 저장매체가 아닌 DVD, Blu-ray등의 분리형 매체에 한해 복사가 가능함.

지하며, 휴대용 사적이용 인증기기가 분실/도난된 경우에도 네트워크 복제를 통한 불특정 다수의 이용을 막을 수 있기 때문에 방송프로그램의 불법 이용 위험도가 낮다. 또한 시나리오 7과 같이 외부 도메인의 방송프로그램을 복사한 후 이용하는 경우, 해당 도메인의 휴대용 사적이용 인증기기를 대여/양도하여 방송프로그램을 이용할 수 있으며, 휴대용 사적이용 인증기기는 무분별한 대여/양도가 불가능하므로 상기 방식은 사용자와 외부 기기의 관계를 기술적으로 구분할 수 없는 환경에서 불특정 다수의 무분별한 이용을 효과적으로 방지할 수 있다.

반면 DVB-CPCM ADM은 리모트 환경에서 사용자가 보유한 방송프로그램을 이용하기 위해 별장(Second-home) 도메인을 이용해야 한다. 그러나 현재의 CPCM 규격에는 리모트 환경의 기기를 별장 도메인으로 등록시키기 위한 절차가 명시되어 있지 않다. 또한 네트워크를 통해 리모트 기기의 이용주체를 인증하는 방법은 외부 인증기관 없이 이루어지기 어려우며, 네트워크의 특성 상 불특정 다수의 접근이 가능한 형태로 악용될 가능성이 높다. 특히 시나리오 3 ~ 6과 같이 공공장소에서의 방송프로그램 이용일 경우, 별장 도메인의 등록이 가능하더라도 방송프로그램을 이용한 후 불특정 다수의 이용자에 의해 방송프로그램이 무단으로 이용될 위험이 있다.

Dubbing10은 현재 DVD, Blu-ray 등의 분리형 매체(Removable Media)와 물리적으로 연결된 기기를 대상으로 방송프로그램 복사를 지원한다. 따라서 물리적으로 연결이 불가능한 외부 기기에서 방송프로그램을 이용하기 위해서는 DVD, Blu-ray 등의 분리형 매체로 방송프로그램을 복사한 후 이를 통해서 이용이 가능하다. 분리형매체는 CPRM(Content Protection for Recordable Media)[5], AACS(Advanced Access Content System)[6] 등의 보호기술이 적용되어 있기 때문에 불법 재배포 위험도는 낮다. 다만 방송프로그램의 복사 경로에 전혀 제약을 두지 않는 제안 기술과는 달리, Dubbing10은 반드시 분리형 매체를 이용하여 방송프로

그램을 이동해야 하고, 분리형 매체를 인식할 수 있는 기기에서만 방송프로그램 이용을 지원하므로 사용자의 불편을 초래한다.

V. 결 론

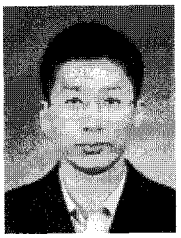
본 논문에서는 휴대용 보안 저장매체를 이용한 방송프로그램의 사적이용 인증방법을 통해 도메인에 등록된 휴대용 사적이용 인증 기기를 보유한 사용자가 물리적인 장소에 구애 받지 않고 자신의 방송프로그램을 자유롭게 사용할 수 있도록 함으로써 사용자의 실제 사적이용을 보장할 수 있는 방법을 제안하였다. 구현을 통해 제안한 방법이 기존 기술로 대응하기 어려운 다양한 시나리오를 지원할 수 있음을 확인하였으며, 특히 사용자의 이용 편의성과 불법 이용을 차단하는 보안성을 동시에 충족해야하는 지상파 방송프로그램 보호기술의 요구사항 측면에서 다른 기술에 비해 월등히 효과적임을 보였다. 본 제안 기술은 향후 방송프로그램 보호 기술로 활용될 수 있을 것이다.

참 고 문 헌

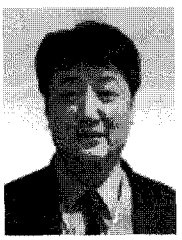
[1] DVB-CPCM Bluebook A94r1, DVB Content Protection and Copy Management, 2007.
[2] Dubbing10, http://home.jeita.or.jp/
[3] 이주영, 추현곤, 남제호, "방송프로그램의 사적이용 지원 기술 연구", 2008 한국멀티미디어학회 추계학술대회 논문집, pp. 590-593, 고려대학교, 2008년 11월
[4] 이주영 외 5인, "지상파DTV 방송프로그램 사적이용 시나리오", ETRI 기술문서, 5225-2008-0056, 한국전자통신연구원, 2008.
[5] 4C Entity CPRM, http://www.4centity.com/
[6] AACS, http://www.aacsla.com/
[7] 차세대방송표준포럼 방송콘텐츠보호관리분과위원회, http://www.nextb.or.kr/subcommi4.html

저 자 소 개

이 주 영(정회원)
2003년 아주대학교 미디어학과 (학사)
2006년 한국과학기술원 전산학과 (석사)
2006년~현재 한국전자통신연구원 방통미디어연구부 연구원
<주관심분야 : 콘텐츠 저작권 보호기술, 콘텐츠 식별 기술, 멀티미디어 데이터베이스>



추 현 곤(정회원)
1998년 한양대학교 전자공학과 (학사)
2000년 한양대학교 전자공학과 (석사)
2005년 한양대학교 전자통신전파공학과 (박사)
2005년~현재 한국전자통신연구원 방통미디어연구부 선임연구원
<주관심분야 : 콘텐츠 보호관리, Contents-base Image/ Video Retrieval, Watermarking, Biometrics>



남 제 호(정회원)
1992년 홍익대학교 전기제어공학과 (학사)
1996년 University of Minnesota, Electrical Eng. (석사)
2000년 University of Minnesota, Electrical Eng. (박사)
2001년~현재 한국전자통신연구원 방통미디어연구부 선임연구원, 융합콘텐츠보호연구팀장
2007년~현재 과학기술연합대학원대학교(UST) 이동통신 및 디지털방송공학과 부교수
<주관심분야 : 신호처리, 디지털방송기술, 멀티미디어 보호관리, MPEG>