IPMP 시스템 사용자 환경의 구현

김장하° 박한성 김상욱
경북대학교 컴퓨터과학과
{jhkim°, hspark, swkim}@woorisol.knu.ac.kr

Implementation of User Environment in IPMP System

Jangha Kim° Hanseong Park Sangwook Kim
Dept. of Computer Science, Kyungpook National University

요 약

인터넷의 확장과 함께 광대역폭을 이용한 다양한 멀티미디어 데이터의 전송이 더욱 가속화 되고 있다. 상용화 추세에 접어들고 있는 멀티미디어 데이터 서비스에서 지적 재산권의 관리와 보호는 컨텐츠 유통에서 반드시 요구되는 사항이다. 컨텐츠에 적용된 보안 체계를 무력화하기 위한 공격자들의 공격 유형이 점점 다양해짐에 따라 사용자 환경 차원에서 새로운 보안요소를 적용하여 단말 재생기의 환경을 제어함으로 악의를 가진 사용자들의 컨텐츠 보안체계 공격을 무력화시키고 안전한 컨텐츠 유통 환경을 제공하는 보안 시스템을 구현한다.

1. 서 론

컨텐츠의 폭발적인 증가와 더불어 해킹기법 또한 다양해지고 있다. 그리고 새로워지는 해킹기법에 대응하여 컨텐츠 보안 기술도 발전하고 있다. 일반적으로 공급자가 새로운 디지털 미디어 컨텐츠를 제작하면 인증과정을 거친 사용자들에게 전달한다. 사용자들은 컨텐츠를 무단 복제하기 위하여 컨텐츠의 보호 장치를 해킹한다. 보호 장치가 제거된 컨텐츠는 P2P 공유 프로그램이나 웹 사이트를 사용하여 전달된다. 이러한 과정으로 복사와 인용이 된 컨텐츠가 인가되지 않은 사용자에게 전달된다. 전통적인 컨텐츠 보안 기법으로 컨텐츠를 보호할 때 컨텐츠의 중요도에 따른 공격 가능성이 높아지면 보안 장치의 견고함에 치명적이다. 새로운 컨텐츠 보안 기법의 등장과 함께 급속도로 번져나가는 형태의 새로운 패러다임의 해킹기법들은 앞으로 더욱 발전하게 될 전망인데 이것을 미연에 방지하기 위하여 새로운 개념의 컨텐츠 보안 시스템인 Intellectual Property Management and Protection이 출연하였다.[1] 이 시스템은 MPEG(Motion Picture Expert Group)에서 사용하는 DRM(Digital Right Management)시스템이다. 멀티미디어와 같은 다양한 컨텐츠에 대한 지적 재산권의 영구적이며 신뢰성있는 관리 및 보호 기능을 제공한다. 비디오와 오디오 컨텐츠의 생성에서 유통과 폐기까지 과정에서 재산권을 관리하며 보호한다. 개별 사용자는 각각의 컨텐츠를 소유하고 인정된 소유권을 기반으로 유통과 폐기한다.

본 논문에서는 이러한 시스템 사용자 환경을 구현하여 IPMP-UE 라고 호칭하였고 시스템을 더욱 효율적으로 사용하기 위하여 윈도우즈 운영체제에서 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서는 IPMP System에 대해서 알아보고 동작 메커니즘을 분석한다. 3장에서는 분석한 IPMP System에서 요구하는 사용자 환경의 효율적인 구현 방법에 대하여 설명한다. 4장에서는 구현된 사용자 환경이 사용된 실험결과를 보여주며, 그리고 5장에서는 결론 및 앞으로의 연구 방향을 제시한다.

2. Intellectual Property Management and Protection System

본 논문에서 Intellectual Property Management and Protection(이하 IPMP)시스템은 구현된 사용자 환경을 단말으로하는 시스템이다. 이 시스템은 크게 컨텐츠를 생성하는 저작도구와 컨텐츠의 소유권과 유통 관계를 관리하는 Contents Verification Agency(이하 CVA), 단말 환경에서 컨텐츠의 유효성 인증과 이용을 담당하는 재생기의 구조로 나누어진다. 이 시스템의 구조를 그림으로 나타내면 그림 1과 같다.

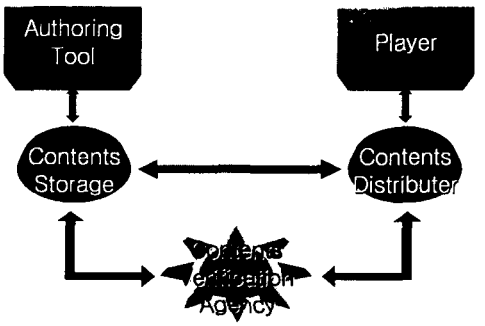

그림 1

2.1 저작도구

저작도구란 비디오 오디오 텍스트와 같은 다양한 형태의 입력 데이터을 이용하여 컨텐츠를 생성하기 위한 프로그램이다. 본 논문에서는 MPEG 저작도구 중에서 광범위한 데이터를 포괄할 수 있는 MPEG-4 저작도구를 실험환경으로 선택하였다.[2] 기존의 MPEG-4에 존재하는 IPMP 아이템을 기반으로 Watermarking 기술이 포함된 DRM시스템을 접합시킨다. 실제 입력 데이터를 MPEG-4 Multiplexer에 입력하기 전에 DRM시스템을 거쳐 인증과 지적 재산권 정보를 가지는 Key를 삽입한다. 삽입과정에서 필요한 인증과 지적재산권 정보를 주고받는 IPMP Agent가 존재한다. 이 과정을 그림으로 나타낸다면 아래 그림 2와 같다.

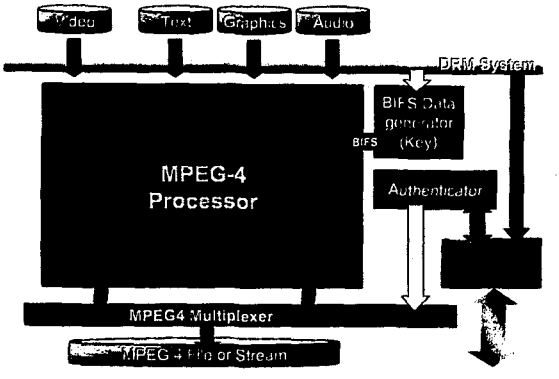

그림 2

2.2 Contents Verification Agency

CVA란 컨텐츠가 생성 유통 폐기되는 과정을 관리하고 통제하는 역할을 하는 에이전트이다. 컨텐츠가 저작도구에 의해서 생성되거나 재생기에 의해서 재생될 때 필요한 라이센스, 인증과 지적재산권의 관리를 위한 Key를 분배 및 검증하기 위한 역할을 한다. Key 분배 알고리즘은 Public Key Infrastructure를 적용시키고 인증에 관련된 여러 가지 데이터를 관리하는 인증기관 역할을 수행한다. 전체 시스템에서 고도의 보안성이 요구되는 부분이며 CVA에 자체의 무결성이 필요하다.[3]

2.3 재생기

재생기란 저작도구에서 생성되거나 다른 여러 가지 단말 환경에서 양도 폐기와 같은 유통 및 인증 과정을 거친 컨텐츠 재생의 위한 프로그램이다. 본 논문에서는 MPEG 재생기 중에서 광범위한 데이터를 포괄할 수 있는 MPEG-4 재생기를 실험환경으로 선택하였다. 기존의 MPEG-4 재생기에서 사용된 DeMultiplexer를 사용하여 포함된 IPMP 정보를 추출하고 MPEG-4 Decoder에 의해 디코딩된 다양한 종류의 컨텐츠에서 저작도구의 DRM 시스템에서 삽입한 인증과 지적 재산권 정보를 가지는 Key를 추출한다. 비디오 오디오 이미지와 같은 형태의 데이터에서는 Watermarking 기술로 저장된 Key를 추출한다. 저작도구에서 존재하는 IPMP Agent와 같은 역할을 하는 Agent가 추출된 정보의 유효성을 검증한다. 인증된 컨텐츠는 정상적인 화면으로 재생되고 인증되지 못한 컨텐츠는 재생이 불가능하게 된다. 이 과정을 그림으로 나타낸다면 아래 그림 3과 같다.[4]

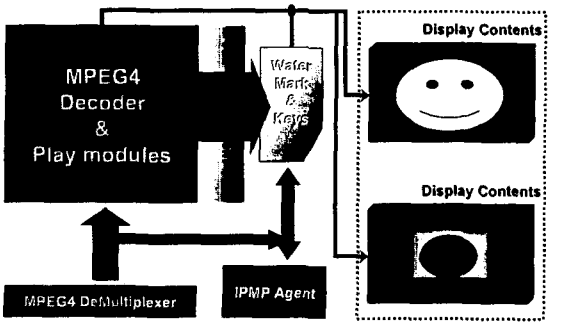

그림 3

3. IPMP-UE(User Environment)

멀티미디어 데이터 보안 체계에 대한 공격의 대부분이 단말에서 이루어진다. 파일 또는 스트리밍 형태로 제공되는 컨텐츠는 다음과 같은 공격 유형에 의해 쉽게 인증되지 않은 사용자에게 배포가능한 형태로 변환된다.[5] 첫번째로 클립보드를 사용한 복사하기와 붙여넣기 기능으로 인터넷을 통해 전달받은 텍스트 컨텐츠를 복사할 수 있다. 두 번째로 윈도우 운영체제가 제공하는 스크린 캡춰 기능을 이용하여 인가된 사용자만 접근할 수 있거나 Watermarked 이미지를 Watermark가 제거된 배포가능한 형태의 이미지로 변형시킬 수 있다. 세 번째로 스트리밍을 통한 실시간 비디오 전송이나 라이센싱 기술을 적용하의 지정된 호스트에서만 비디오를 재생할 수 있도록 한 경우, 윈도우의 특정 화면 영역을 비디오 캡춰할 수 있는 프로그램을 사용하여 배포가능한 형태의 비디오로 변형시킬 수 있다. 마지막으로 HTTP 프로토콜 자체가 가진 개방형 특성을 이용한 인증 우회기법으로 컨텐츠를 인증되지 않은 사용자가 접근할 수 있다.

인터넷을 통한 컨텐츠 전송 중 공격인 스니핑 스푸핑 하이재킹은 CVA에 의해 인증된 재생기에서만 재생이 가능하므로 IPMP시스템으로 차단할 수 있다. 하지만 인증된 재생기를 사용하는 단말에서 전송받은 멀티미디어 데이터 보안체계에 대한 공격이 이루어진다면 사용자 환경에서는 강력한 보완체계가 필요하다. 다음 조건을 만족하는 재생기의 사용자 환경이 요구된다. 키보드 마우스와 같은 직접입력장치에 대한 제어기능과 프로세스와 운영체제 수준에서의 캡춰프로그램 탐지 및 자동화된 프로세스 실행기의 제어기능이 요구된다.

본 논문에서는 마이크로소프트 윈도우를 사용자 환경

의 실험환경으로 선택하여 실제 IPMP시스템의 단말 사용자 환경의 요구사항을 지원할 수 있는 IPMP-UE를 구현하였다.

4. 구현 및 실험결과

본 장에서는 제안된 IPMP-UE를 적용시키기 전 취약한 멀티미디어 컨텐츠의 재생기 환경과 적용된 후 환경을 앞서 언급된 세가지 공격 유형으로 실험한 결과를 비교, 분석한다.

IPMP-UE의 실험은 파일로 저장된 컨텐츠를 대상으로 이루어졌다. 재생기 환경에서 IPMP-UE가 제안하는 직접 입력장치와 프로세스제어기능을 적용 전 환경과 적용 후 환경으로 나누어 실험하였다. 각각의 환경에서 컨텐츠를 무단 복제하기 위하여, 앞서 언급한 공격유형을 사용하여 공격하였다. 실제 복제된 컨텐츠를 생성가능 할 경우 'O'로 표시하였고 생성 불가능할 경우 'X'로 표시하였다. 공격1은 일반적인 클립보드를 통한 공격이며, 공격2는 스크린 캡춰를 이용한 공격이다. 공격3은 레코딩 프로그램을 이용한 공격이다. IPMP-UE를 실험한 결과는 표 1과 같다.

	일반 단말 환경			IPMP-UE		
	공격1	공격2	공격3	공격1	공격2	공격3
텍스트	O	O	O	X	X	X
이미지	O	O	O	X	X	X
오디오	X	X	O	X	X	X
비디오	X	X	O	X	X	X

표 1

표 1의 경우를 살펴보면 IPMP-UE가 단말 재생기에 적용될 경우 무단복제를 위한 공격시도를 차단할 수 있음을 보였다. IPMP시스템의 목적 중 하나는 컨텐츠의 무단배포 방지를 위한 것에 있다. 이것은 전체 시스템에서 각각의 구성요소들이 보안요소를 갖추어야만 가능하다. 그 중에서 IPMP시스템 단말환경 IPMP-UE는 사용자 환경에서 컨텐츠 무단 복제와 같은 공격시도를 차단할 수 있도록 도움을 줄 수 있다.

5. 결론 및 향후 연구 방향

본 논문의 IPMP시스템 사용자 환경은 컨텐츠의 안전한 유통을 위한 단말 환경에서의 보안 시스템이다. IPMP 시스템은 컨텐츠의 저작도구 CVA 재생기가 조화를 이루어야 한다. 재생기는 인가된 사용자 환경에서 동작하지만 인가되지 않는 사용자로의 무단배포를 목적으로 컨텐츠의 보안체계가 공격받고 있다. 단순한 재생기와 컨텐츠의 보안성으로 해결할 수 없는 요소들이 많다. 운영체제의 입력장치 제어와 공격프로세스 탐지 기법을 통하여 새로운 사용자 환경에 구성하였다. 이를 사용하여 단말 환경에서 실제 컨텐츠 공격을 차단할 수 있었고 IPMP시스템의 대한 보안성을 한단계 더 확보할 수 있었다. 이 점은 IPMP시스템 전체의 보안성의 향상에도 기여했다고 본다.

제안된 IPMP시스템과 IPMP-UE가 안정적으로 수행되어지기 위해서는 더욱 보강되어야 할 점들이 있다.[6] 우선 더 다양한 운영체제와 컴퓨팅환경에서 사용자 환경 제어가 가능하도록 보완할 필요성이 있다. 그리고 다양한 컨텐츠를 수용할 수 있는 MPEG-4시스템에 적용할 수 있는 전체 IPMP 시스템을 구현해야할 것이다.[7] 이를 위해서는 MPEG-4시스템에 대한 분석과 DRM시스템에 대한 이해가 필요하다. 본 논문은 전체 IPMP시스템의 구현에서 시작점이 된다.

MPEG-21에서 지향하는 컨텐츠 유통은 컨텐츠 보안이 불가결한 요소이다. IPMP시스템은 컨텐츠 유통과 함께 연동되어야 하며 거대한 컨텐츠 유통 인프라에 내포되어 있어야 한다. 컨텐츠의 증가는 컨텐츠의 생성 유통 폐기에 소요되는 비용도 증가시킨다. 컨텐츠 보안은 이러한 비용을 효율적으로 절감시키고 무단유포와 같은 경제적 손실을 방지할 수 있다.

전체 IPMP시스템에서 고려되어져야할 네트워크로 배포되는 컨텐츠에 대한 위협요소들이 많다. 하지만 아직까지 단말 환경에서 컨텐츠에 대한 공격시도가 컨텐츠 보안에서 더욱 위협적인 존재이다. 단말환경에서 컨텐츠 대한 최신 공격 기법에 대응할 수 있는 신속하고 효과적인 방어 기술 연구가 더욱 더 진행되어야 할 것이다.

참고문헌

[1] JTC 1/SC 29/WG11 N4270, "MPEG-4 Sysyem - IPMP Information" ISO/IEC 2001

[2] Fernando Pereira and Touradj Ebrahimi, "MPEG-4 book" MPEG-4 Objectives Overview p1-61 2002

[3] Johannes A.Bushmann, "Introduction to cryptography" Identification Public-Key Infrastructure p241-256 2001

[4] Atul Puri and Tsuhan Chen, "Multimedia Systems, Standards, and Networks" MPEG-4 Players implementation 2000

[5] Yao Wang and Jorn Ostermann and Ya-Qin Zhang, "Video processing and communications" Coding of Audio visual Objects with MPEG-4 p437-454 2002

[6] JTC1/SC29/WG11 N4323, "Request for addition of a Part 4 to ISO/IEC 21000 (Intellectual Property Management and Protection)" ISO/IEC 2001

[7] JTC1/SC29/WG11 W4271, "Analysis of Compliance with Requirements of the IPMP Extensions" ISO/IEC 2001