퍼즐 인증 프로토콜을 이용한 DRM 시스템에 관한 연구

정용훈[†] · 이광형[††] · 민소연[†††] · 전문석[††††]
숭실대학교 컴퓨터공학과[†], 서일대학 인터넷정보과[††]
서일대학 정보통신과[†††], 숭실대학교 컴퓨터공학과[††††]
s0178,@ssu.ac.kr, dreamace@seoil.ac.kr, symin@seoil.ac.kr
mjun@computing.ssu.ac.kr

A Study on DRM System using Puzzle Authentication Protocol

Young-Hoon Jung[†] · Kwang-Hyoung Lee[††] · Min-So Yeon[†††] · Moon-Seog Jun[††††]
Dept. of Computer Engineering, Soongsil University[†]
Dept. of Internet Information, Seoil College[††]
Dept. of Information Communication, Seoil College[†††]
Dept. of Computer Engineering, Soongsil University[††††]

요 약

본 논문에서는 첫째, 기존의 단순 One-path XOR 방법보다 안전한 M * N Puzzle 기법을 이용한 Key 전송방법을 제안한다. 둘째, 생성된 Puzzle은 서버에 저장하지 않으므로 기존의 시스템보다 보안성이 높은 방법을 제안한다. 셋째, 클라이언트에서 복호화 할 때 OTP와 함께 Puzzle을 복호화 하는 클라이언트 복호화 시스템을 제안한다. 넷째, M * N Puzzle기법과 OTP를 조합으로 보다 안전한 키 전송을 제안한다.

키워드 : 디지털 저작권 관리, 원타임 패스워드, 퍼즐 암호화, 대칭키

Abstract

In this paper, I suggest that as follow. First, it is the algorithm to transmit the encryption key which use M * N Puzzle method more safe than the existing One-path XOR method. Second, it does provide the high quality of security than the existing system because it does not save the generated puzzle to the server side. Third, it does support the client decryption system which can decrypt the puzzle with OPT in decryption with client side. Fourth, it does adopt more of the safe transmission method with the compound of M * N puzzle method and OPT.

Keyword : DRM, OTP, Puzzle Encryption, Symmetric Key

I. 서 론

인터넷의 확산과 컴퓨터 상호연결성의 증대로 디지털 자원에 대한 유통 환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 멀티미디어 자료에 대한 수요가 급격하게 증가하고 있다. 디지털 저작물은 품질에 손상 없이 복제와 배포가 가능하기 때문에 디지털 저작권

본 연구는 서울시 산학연협력사업으로 구축된 서울 미래형 콘텐츠컨버전스 클러스터 지원으로 수행되었습니다.

관리(DRM: Digital Rights Management) 기술을 통해 디지털 저작물에 대한 지적재산권 침해사례로부터 저작권을 보호하고, 유통과정을 관리하기 위한 종합적인 대책이 추진되어 저작물 제작, 유통, 이용 등이 일련의 신뢰할 수 있는 환경에서 이루어질 수 있도록 하는 다양한 연구가 진행 중에 있다[3]. 이러한 DRM 기술을 이용하여 Microsoft사와 InterTrust사 등의 외국 업체와 국내의 Digicap 같은 국내 여러 업체가 다양한 형태의 DRM 솔루션을 제공하고 있다.[1]

하지만 기존 DRM 솔루션은 암호화와 복호화에 사용하는 키가 사용자에 의하여 노출되면 저작물에 대한 보호는 더 이상 보장하지 못하는 단점을 가지고 있다.

기존의 DRM의 문제점을 해결하기 위해서 Puzzle 기법과 OTP(One Time Password)를 제안하며, 암호화의 보안성을 높이기 위해 Puzzle기법과 OTP 두 가지를 이용하여 암호화하는 방법을 제안한다. 복호화는 E-mail과 Mobile phone을 이용하여 Puzzle기법과 OTP를 사용자에게 전송하여 사용자 인증을 하는 시스템을 제안하였다.

II. 관 련 연 구

2.1 기존의 DRM 시스템

2.1.1 InterTrust의 DRM 시스템

InterTrust사의 DRM 솔루션은 사전에 암호화되어 배포되므로 사용자의 컴퓨터에서 저작물을 사용하는 시점에서 라이선스 에이전트가 라이선스를 획득하고 지불정보를 전송하여 거래를 체결하도록 하였다.[1] 또한 저작물이 암호화로 보호되고 있으므로 사용자들 사이에 암호화된 저작물을 주고받을 수 있는 저작물 재분배(SuperDistribution)를 실현하였다.[2]

하지만 InterTrust사의 DRM 시스템의 복호화는 복호화가 끝난 후에 재생이 가능한 점, 한 개의 키로만 암호화되기 때문에 키 유출시 더 이상 보호를 받지 못한다는 점, 파일 전체를 암호화하기 때문에 암호화/복호화 시간이 올래 걸린다는 단점을 가지고 있다.

2.1.2 Microsoft의 DRM

Microsoft의 DRM 시스템은 WMRM(Windows Media Rights Manager)으로서 저작물 제공자에게 인터넷상에서 암호화된 파일 형식으로 미디어를 배달한다. WMRM에서 각각의 서버 또는 클라이언트 인스턴스들은 개인화(indivisualization)과정을 통해 키쌍을 할당받게 되며, 크래킹 되었거나 안전하지 않다고 판단되는 인스턴스에 대해서는 인증서 취소목록을 이용하여 서비스 대상에서 제외시키게 된다.

하지만 Microsoft사의 DRM은 자사의 WMV와 WMA의 파일 포맷만을 지원하고, 암호화시 파일 전체를 인코딩하여 암호화하기 때문에 시간이 오래 걸린다.

III. 제안하는 시스템

3.1 제안하는 DRM 시스템 암호화 방법

본 논문에서 제안하는 시스템은 M*N 크기의 Puzzle을 이용하여 온라인상에서 디지털 콘텐츠에 대한 사용자 인증과 암호화를 통해 불법적인 실행 및 수정을 방지할 수 있는 DRM 시스템으로 DRM Server는 Client와 사용자를 인증함으로서 기존의 단순 유·무선 조합 인증기법보다 안전성이 향상 되었다.

DRM Server에서는 Puzzle를 이용하여 콘텐츠를 암호화하고 이를 사용자에게 전송한다. 제안하는 시스템의 구성은 (그림1)과 같다.

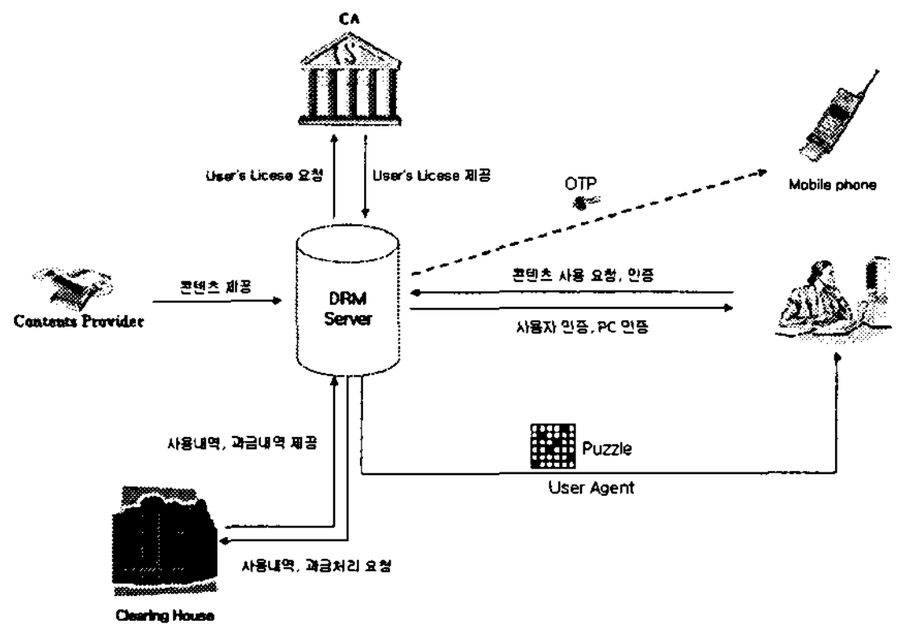

그림 1. 제안하는 시스템 구성

Client는 DRM Server에 접속하여 Agent를 설치하고 원하는 콘텐츠의 검색 및 다운 요청을 한다. DRM Server에서는 콘텐츠 사용 요금 지불 요청과 함께 콘텐츠를 전송하며, 사용자는 요금을 지불한 사실과 함께 콘텐츠 실행 요청을 보내게 된다. DRM Server는 요금 지불이 완료된 사용자에게 M*N Puzzle과 OTP를 각각 유·무선을 통하여 전송하고 사용자는 DRM Server로부터 받은 M*N Puzzle과 OTP를 이용하여 Puzzle을 복호화고 콘텐츠를 재생하게 된다.

3.2 제안하는 Puzzle 암호화 복호화 기법

3.2.1 Puzzle 암호화 기법

DRM Server에서는 Client로부터 콘텐츠 사용 요청이 들어오면 암호화키를 XOR 기법을 이용하여 두 개의 키로 나눈다. 이렇게 두 개의 키로 분리된 암호화키를 Puzzle 1행과 10행에 배치하고 나머지는 랜덤값으로 패딩(Padding)하고 변형된 Puzzle과 Puzzle 조합도를 Agent를 통하여 Client로

전송된다. Puzzle 조합도를 복호화 하기 위한 값은 OTP 값으로 사용자의 Mobile phone으로 전송한다.(그림 2)

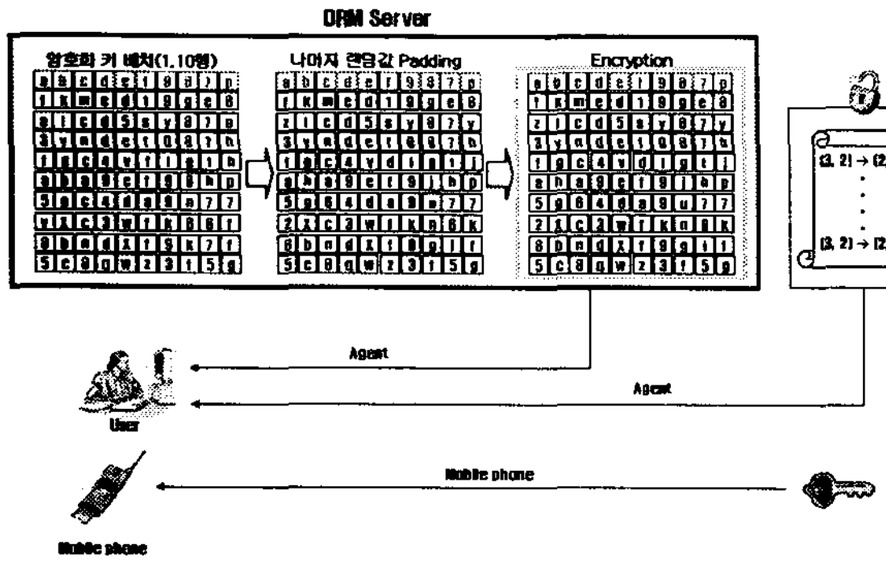

그림 2. Puzzle 암호화 기법

사용자는 이렇게 유·무선을 통하여 DRM Server로부터 전송받은 Puzzle과 OTP를 이용하여 Puzzle을 복호화하고 암호화키를 획득하여 콘텐츠를 재생한다.

3.2.2 Puzzle 복호화 기법

Puzzle 복호화는 DRM Server로부터 다운 받은 콘텐츠와 Puzzle, Puzzle 조합도, OTP를 이용하여 복호화를 수행한다. 복호화 과정은 암호화 기법의 역순으로 진행된다.(그림 3)

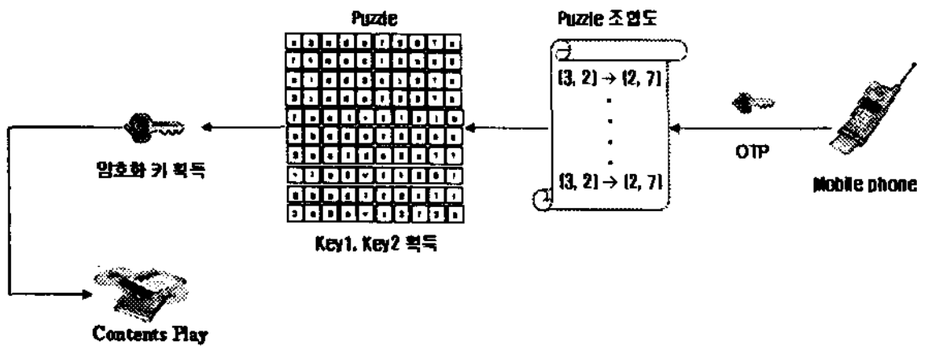

그림 3. M*N Puzzle 복호화 기법

복호화 과정을 보면 먼저 Mobile phone으로 전송받은 OTP값을 이용하여 Puzzle 조합도를 복호화 하게 된다. 이렇게 복호화된 Puzzle 조합도를 이용하여 Key1과 Key2 값을 Puzzle에서 추출하고, Key1과 Key2 값을 XOR하여 암호화키를 획득하게 된다.

이때 OTP값과 Puzzle, Puzzle 조합도는 복호화를 수행할 때마다 새롭게 DRM Server로부터 전송받아야 한다.

이렇게 획득한 암호화키로 사용자는 멀티미디어 콘텐츠를 재생시킬 수 있다.

IV. 실 험 평 가

4.1 기존 시스템과의 비교 분석

DRM 시스템은 유선 환경만을 이용하여 키 분배를 하며, I사는 공개키로 암호화하여 전송하며, M사의 경우 복호화 키를 전송한다. 또한 키 재요청시 동일한 키를 전송한다. 기존의 DRM 시스템과 제안하는 시스템의 차이는 유·무선 모두를 사용하며, 키 재요청시 새로운 키를 생성하여 전송하게 된다.

제안하는 시스템은 키 분배 방법은 유선으로 Puzzle과 Puzzle 조합도를 보내며, 무선을 이용하여 OTP를 전송하여 보안성을 높였다. 키 분배 환경과 분배 방법, 재전송에 대한 비교는 (그림 4)를 보면 기존 DRM 시스템과 제안하는 시스템을 비교해 볼 수 있다.

비교	기존I사 DRM	기존M사 DRM	제안하는 시스템
PKI 사용 여부	Y	N	N
키 분배 환경	유선	유선	유/무선
키 분배 방법	공개키로 암호화 후 전송	복호화 키 전송	Puzzle, Puzzle 조합도, OTP 전송
키 재요청 시	동일 값 전송	동일 값 전송	새로운 값 전송
Sniffing 가능 여부	Y	Y	N
복호화 키 노출 여부 (Sniffing 시)	N (본인이 아니면 복호화키 추출 불능)	Y (복호화 키 유출, 보호대책 없음)	N (복호화 키 생성 불가능)

그림 4. 기존 DRM과 제안하는 시스템

I사는 PKI를 사용 유선환경에서 공개키로 암호화하여 전송하였고 키 재전송 요구시 동일한 값을 전송한다. M사는 PKI 환경이 아니며, 유선환경을 이용하여 복호화키를 전송하며, 키 재전송 요구시 동일한 복호화키를 재전송 한다.

제안하는 시스템은 유·무선 환경을 이용하여 사용자에게 재배치된 Puzzle과 Puzzle조합도, OTP를 전송한다. 키 재전송 요구시 새로운 Puzzle과 Puzzle조합도, OTP가 모두 재전송된다.

기존의 시스템과 제안하는 시스템과의 전반적인 사항을 비교 분석 해 보면 제안하는 시스템은 기존 시스템과 같이 유선 환경을 지원하며 동시에 무선 환경을 이용하여 사용자 인증에 있어 기존의 시스템보다 더 향상되었다.

V. 결 론

본 논문에서는 유·무선을 이용하여 보다 안전한 키를 전송하여 멀티미디어 콘텐츠를 보호하는 시스템을 제안하였다.

제안하는 시스템은 유선으로 전송되는 Puzzle이 유출되어 불법적인 사용자가 볼 수 있어도 복호화 할 수 없다. Puzzle을 복호화하기 위해서는 무선으로 전송되는 OTP값이 있어야 한다.

무선으로 전송되는 OTP는 OTP(One Time Password)와 같이 사용시간을 두어 일정 시간이 지나면 효력이 없어져 다시 전송을 받아야 한다. 이렇게 유·무선을 이용하여

Puzzle과 OTP를 전송하고 유선으로 전송되는 Puzzle이 유출되어도 무선으로 전송되는 OTP가 없이는 복호화가 불가능하게 하였다.

향후 과제는 Puzzle 기법과 휴대폰 및 PDA와 같은 이동식 휴대 단말기에서 활용할 수 있도록 시스템을 개선할 계획이다.

참 고 문 헌

[1] 이광형 외 4명, "다중 랜덤 대칭키를 사용한 DRM 보안 시스템에 관한 연구,"한국정보처리학회 2005년 추계학술대회 VOL. 12 NO. 02 pp. 0893~896 2005.11

[2] 김정재 외 2명, "동영상 데이터 보호를 위한 공유키 풀 기반의 DRM 시스템," 한국정보처리학회 논문지 C, VOL. 12-C NO. 2pp. 0183~0190 2005.04

[3] Sung, J Park, "Copyrights Protection Tech niques," Proceedings International Digital Content Conference, Seoul Korea, Nov. 28-29, 2000.

[4] 정용훈 외 2명, "멀티미디어 데이터 보호를 위한 랜덤 대칭키 기반 부분 암호화 시스템," 한국정보과학회 한국컴퓨터종합학술대회 VOL. 00 NO 00pp. 0154~0156 2005.07

[5] 추연수 외 1명, "DRM 시스템을 위한 안전한 복호화 키 분배 시스템 설계" 한국정보과학회 한국컴퓨터종합학술대회 VOL. 00 NO. 00 pp 0157~0159 2005.07

[6] Microsoft : http://www.microsoft.com/windows/windowsmedia/drm.asp

[7] Joshua Duhl, "Digital Rights Management : A Definition," IDC 2001.

[8] Joshua Duhl and Susan Kevorkian, "Unde rstanding DRM system: An IDC White paper," IDC, 2001

[9] Intertrust : http://www.intertrust.com/main/overview/drm.html