멀티미디어 콘텐츠 보호를 위한 향상된 인증 프로토콜 보안 시스템에 관한 연구

이광형*, 정용훈**, 이영구**, 김현철**, 전문석**
*서일대학, **숭실대학교 컴퓨터공학과
dreamace@seoil.ac.kr, {s0178, ad3927, dmzpolice}@ssu.ac.kr
mjun@computing.ssu.ac.kr

A Study on DRM System for Multimedia Contents Protection base on Advanced Authentication Protocol

Kwang-Hyung Lee*, Young-Hoon Jung**, Young-Gu Lee*,
hyun-chul Kim, Moon-Seog Jun***,

요 약

본 논문에서는 디지털 콘텐츠의 암호화를 Puzzle기법을 사용하여 Puzzle을 재배치하고 재배치한 조합도를 공개키로 암호화 하여 유선을 통하여 전송하고, 조합도 암호화키 OTP를 생성하여 무선으로 사용자에게 전송하는 알고리즘을 제안하고, 재배치된 Puzzle기법과 Puzzle조합도 및 OTP를 E-mail과 Mobile phone을 이용하여 높은 수준의 사용자 Deviec와 사용자 인증을 제안하였다. 제안 시스템을 설계하고 구현한 후 성능 평가를 위해 다양한 콘텐츠 파일을 이용하여 실험을 수행하여 제안한 시스템이 기존 시스템에 비해 높은 보안성을 검증하였다.

1. 서론

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 관리(DRM: Digital Rights Management) 기술이 필요하다. 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 단점이 있다.

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

2. 관련연구

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 취소 목록을 이용하여 서비스 대상에서 제외시키게 된다.

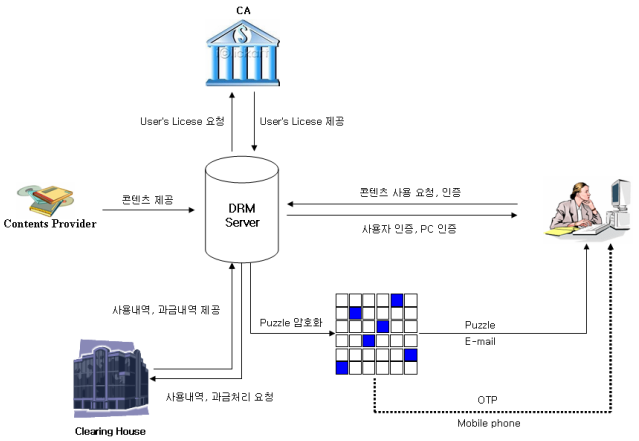
하지만 Microsoft사의 DRM은 자사의 WMV와 WMA의 파일 포맷만을 지원하고, 암호화시 파일 전체를 인코딩하여 암호화하기 때문에 시간이 오래 걸린다.

3. 제안하는 시스템

3.1 제안하는 DRM 시스템 암호화 방법

본 논문에서 제안하는 시스템은 M*N 크기의 Puzzle 기법을 이용하여 온라인상에서 디지털 콘텐츠에 대한 사용자 인증과 암호화를 통해 불법적인 실행 및 수정을 방지할 수 있는 DRM 시스템으로 Client와 사용자를 인증하여 기존의 단순 유무선 조합 인증기법보다 안전성을 향상 하였다.

DRM Server에서는 Puzzle를 이용하여 콘텐츠를 암호화하고 이를 사용자의 E-mail과 Mobile phone으로 전송하여 Client와 사용자 인증을 한다. 제안하는 시스템의 구성은 (그림1)과 같다.



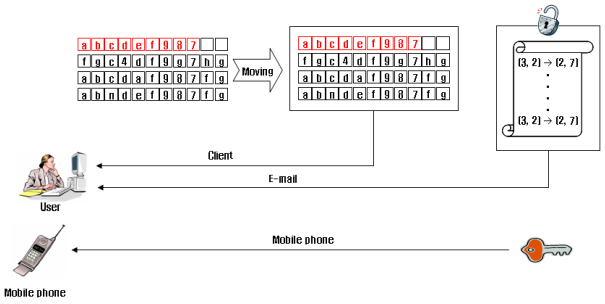
(그림) 1 제안하는 시스템 구조

사용자는 DRM Server에 접속하여 Agent를 설치하고 콘텐츠의 검색 및 다운 요청을 한다. DRM Server에서는 콘텐츠 사용 요금 지불 요청과 콘텐츠를 전송하며, 사용자는 콘텐츠 실행 요청을 보내게 된다. DRM Server는 요금 지불이 완료된 사용자에게 Puzzle과 Puzzle 조립도를 유무선을 통하여 전송하게 되고 사용자는 이를 이용하여 콘텐츠를 복호화하여 재생하게 된다.

3.2 제안하는 Puzzle 암호화 복호화 기법

3.2.1 Puzzle 암호화 기법

DRM Server에서는 콘텐츠 사용 요청이 들어오면 암호화키를 Puzzle를 이용하여 Relocation하고 이렇게 변형된 Puzzle을 Agent를 통하여 Client로 전송된다. Puzzle 조합도는 암호화 하여 사용자의 E-mail로 전송하고, 이렇게 조합도를 암호화한 키는 사용자의 Mobile phone로 전송한다.(그림 2)



(그림 2) Puzzle 기법 암호화 방법

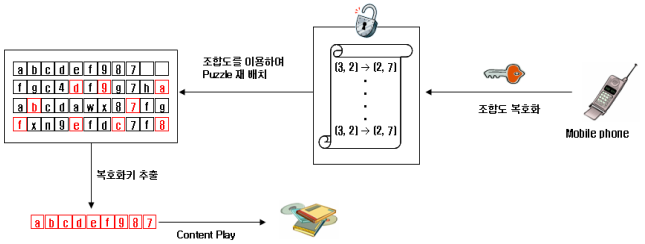
사용자는 이렇게 유무선을 통하여 DRM Server로 전송받은 Puzzle과 조합도, 암호화키를 이용하여 복호화하여 콘텐츠를 재생한다.

Puzzle에는 콘텐츠 암호화키와 콘텐츠의 사용기

간, 사용횟수 등을 같이 암호화하여 사용자가 오프라인 상태에서 콘텐츠의 사용기간과 사용횟수를 기록하여 온라인 상태가 되었을 때 콘텐츠 사용을 제안하거나 요금 지불을 요청할 수 있다.

3.2.2 Puzzle 복호화 기법

Puzzle 복호화는 DRM Server로부터 다운 받은 콘텐츠와 Puzzle, 조합도, 조합도 암호화키를 이용하여 복호화 한다. 복호화 과정은 암호화 기법의 역순으로 진행된다.[그림 3]



(그림 3) Puzzle 기법의 복호화

복호화 과정을 보면 먼저 Mobile phone로 전송받은 키를 이용하여 E-mail로 수신된 Puzzle과 Puzzle 조합도 중 Puzzle 조합도를 먼저 복호화하고 이 Puzzle 조합도를 이용하여 Puzzle을 재배치하여 콘텐츠 암호화키를 추출하여 콘텐츠를 복호화 한다.

4. 실험평가

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 조합도를 보내면, 무선을 이용하여 사용자의 Mobile phone으로 조합도 암호화키를 공개키로 암호화하여 전송하여 보안성을 높였다. 키 분배 환경과 분배 방법, 재전송에 대한 비교는 [그림 4]을 보면 기존 DRM 시스템과 제안하는 시스템을 비교해 볼 수 있다.

비고	기존 I사 DRM	기존 M사 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	복호화 키 분할 후 전송
키 재 요청 시	동일 값 전송	동일 값 전송	랜덤 값 전송
Sniffing 가능 여부	Y	Y	Y
복호화 키 노출 여부 (Sniffing 시)	N (본인이 아니면 복호화키 추출 불능)	Y (복호화 키 유출, 보호하지 못함)	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, 조합도 암호화키를 전송한다. 키 재전송 요구시 새로운 Puzzle과 Puzzle조합도, 조합도 암호화키가 모두 재전송된다.

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

5.결론

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

제안하는 시스템은 유선으로 전송되는 Puzzle과 Puzzle 조합도를 불법적인 사용자가 볼 수 있어도 복호화 할 수 없다. Puzzle 조합도를 복호화하기 위해서는 무선으로 전송된 Puzzle 조합도 복호화키가 있어야만 조합도를 복호화 할 수 있다.

무선으로 전송되는 Puzzle 조합도 복호화 키는 OTP(One Time Password)와 같이 사용시간을 두어 일정 시간이 지나면 효력이 없어져 다시 전송을 받아야 한다. 이렇게 유·무선을 이용하여 사용자 Device와 사용자 인증을 보다 강력하게 하였다.

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

참고문헌

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

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

[4] Brad Cox, Superdistribution : Objects As Property on the Electronic Frontier, Addision-Wesley, May 1996.

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

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

[7] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory, Vol.IT-22, No6, pp.644-654, November 1976

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

[9] V.K. Gupta, "Technological Measures of Protection," Proceedings of International Conference on WIPO, Seoul Korea, October 25-27, 2000.

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