멀티미디어 콘텐츠 보호를 위한 인증 프로토콜

정용훈*, 이광형**, 김정재*, 전문석*
*숭실대학교 컴퓨터학과
**서일대학교 인터넷정보과
e-mail:s0178@ssu.ac.kr

Multimedia Contents Protection based on Advanced Authentication Protocol

Yongl-Hoon Jung*, Kwang-Hyung Lee**,
Jung-Jae Kim*, Moon-Seog Jun*
*Dept. of Computer Engineering, Soongsil University
**Dept. of Internet Information, Seoil College

요 약

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

1. 서론

인터넷의 확산과 컴퓨터 상호연결성의 증대로 디지털 자원에 대한 유통 환경이 급속히 변화함에 따라 온라인 음악, 동영상, e-Book 등 디지털콘텐츠의 유통이 활발해지면서 디지털콘텐츠 산업이 미래의 핵심 산업으로 각광을 받았으나 P2P 등의 무차별 공유 서비스로 인해 디지털콘텐츠 산업은 오랜 기간 동안 정체상태를 벗어나지 못하고 있다. 이러한 디지털콘텐츠의 불법복제 기승으로 인해 기존 오프라인 또는 아날로그 콘텐츠의 유통 구조를 장악하던 음반사 또는 영화제작사 등은 심한 타격을 받게 되었으며, 이들 콘텐츠 공급자들은 궁여지책으로 P2P 사이트에 대하여 불법복제 조장이라는 명목으로 소송을 제기하는 한편 인터넷을 통한 어떠한 형태의 디지털콘텐츠 유통 서비스도 강하게 반발하고 있다. 그러나 콘텐츠의 유통 구조가 기존의 오프라인 또는 아날로그 콘텐츠에서 디지털콘텐츠로 전환되어 가는 추세를 피할 수 없다는 인식하에 품질의 손상 없이 복제가 가능한 저작물의 불법복제 방지를 위한 디지털 저작권 보호문제가 중요한 이슈로 대두되고 있다.

디지털 저작물 보호를 위해서는 안정성과 보안성 확보를 위하여 정보보호 기술이 필요하고, 디지털 저작권과 저작물 유통의 전반을 감시하고 추적하기 위한 디지털 저작권 관리(DRM: Digital Rights Management) 기술이 필요하다[2]. 기존 DRM 솔루션들은 암호화에 사용하는 키로 비밀키를 사용하여 사용자가 파일을 다운로드할 때 암호화를 수행하므로 많은 시간이 소요가 되며, 복호화를 수행하는 경우에도 대용량의 저작물인 경우 전체 파일에 대하여 복호화를 먼저 수행한 후에 실행을 할 수 있으므로 사용자가 실시간으로 파일을 플레이해서 볼 수 없는 문제점이 있었다. 또한 암호화와 복호화에 사용하는 키가 사용자에 의하여 노출이 된다면 해당 저작물에 대한 보호는 더 이상 보장하지 못하는 단점이 있다.

기존의 DRM은 이 문제를 해결하기 위해서 매트릭스 Puzzle 프로토콜을 사용하여 온라인상에서 멀티미디어 저작물에 대한 사용자 인증과 데이터 자체의 암호화를 통해 불법적인 실행을 방지할 수 있는 통합적인 DRM 시스템을 제안한다.

2. 관련 연구

2.1 DRM 연구 현황

디지털 저작물은 품질의 손상 없이 복제가 가능하기 때문에 불법복제로부터 저작자를 보호하기 위해 안전한 디지털 저작권 보호시스템의 개발이 필요하며, 이를 보완하기 위하여 허가되지 않은 사용자로부터 디지털 저작물을 안전하게 보호함으로써 저작권자의 권리 및 이익을 지속적으로 보호하는 다양한 연구가 진행 중에 있다.

2.2 기존의 DRM 시스템과 키 교환 프로토콜

2.2.1 InterTrust의 DRM 시스템

InterTrust사의 DRM 솔루션 특징은 저작물의 보호를 위해서 암호기술과 워터마킹을 사용하며 저작물 사용규칙을 지정하여 사용내역의 수집 및 기록, 과금 처리를 수행하는 것이다. 사용자 컴퓨터에 에이전트를 실행하여 라이선스와 과금 처리, 저작물의 실행을 에이전트를 통하여 처리하도록 하였다. 저작물은 사전에 암호화되어 배포되므로 사용자의 컴퓨터에서 저작물을 사용하는 시점에서 라이선스 에이전트가 라이선스를 확인하고 지불정보를 전송하여 거래를 체결하도록 하였다. 그러므로 신용카드나 전자 화폐 등의 결제 방식을 이용하여 거래할 수 있다[4,5]. 또한 저작물이 암호화되어 보호되고 있으므로 사용자들 사이에 암호화된 저작물을 주고받을 수 있는 저작물 재분배(SuperDistribution)를 실현하였다[3].

그러나 InterTrust사의 DRM 시스템의 복호화는 복호화가 끝난 후에 재생이 가능하다. 또한 한개의 키로만 암호화 하므로 키가 유출이 될 경우 더 이상 보호를 받지 못한다는 점과 파일 전체를 암호화하기 때문에 암호화와 복호화 하는데 시간이 다른 시스템보다 오래 걸리는 점과 재생시 전체 복호화가 끝난 후에야 재생이 되는 단점을 가지고 있다.

2.2.2 Microsoft의 DRM 시스템

Microsoft의 DRM 시스템은 저작물 제공자와 소비자들에게 디지털 미디어 파일을 안전하게 분배하는 종단 간(end-to-end) DRM 시스템이다[6]. 핵심 제어 부분은 WMRM(Windows Media Rights Manager)으로서 저작물 제공자에게 인터넷 상에서 암호화된 파일 형식으로 보호된 디지털 콘텐츠를 배달한다. WMRM에서 각각의 서버 또는 클라이언트 인스턴스들은 개인화(indivisualization)과정을 통해 키 쌍을 할당받게 되며, 크래킹 되었거나 안전하지 않다고 판단되는 인스턴스에 대해서는 인증서 취소목록을 이용하여 서비스 대상에서 제외시키게 된다. 인증서 취소목록은 마이크로소프트사의 웹사이트를 통해 배포된다. 키는 라이선스에 포함되고, 라이선스와 저작물은 분리되어 분배된다.

그러나 Microsoft사의 DRM 시스템의 경우는 자사의 WMV와 WMA의 파일 포맷만을 지원하기 때문에 암호화시 파일 전체를 인코딩하여 암호화하기 때문에 시간이 오래 걸린다.

2.2.3 인증 및 키 교환 프로토콜에 필요한 보안

인증 및 키 교환프로토콜에 필요한 기본적인 요구사항은 다음과 같다.

(1) 개체 인증(entity authentication)

키 교환 프로토콜에 참여하고 있는 상대방의 신원을 확인할 수 있어야만 한다.

(2) 키 확인(key confirmation)

키 교환 프로토콜에 참여한 사용자가 자신이 의도한 상대방과 동일한 세션키를 실제로 공유하였음을 확인할 수 있어야만 한다.

(3) 묵시적 키 인증(implicit key authentication)

세션키의 소유 여부가 알려져 있지 않은 경우라도 키 교환 프로토콜에 참여한 사용자 이외에 어느 누구도 세션키를 계산할 수 없음을 보장해야 한다.

(4) 키 신규성(key freshness)

세션마다 새로운 키를 설정해야만 한다.

(5) 능동적 위장 공격(active impersonation attack)

공격자가 자신을 임의의 다른 사용자로 위장하여 프로토콜에 참여한 후, 정당한 사용자와 키 교환을 성공적으로 수행하는 공격이 불가능해야만 한다.

(6) 완전한 전향적보안성(perfect forward secrecy)

키 교환 프로토콜에 참여하는 사용자간에 장기간 비밀키(long term secret key)가 노출되거나 분실된 경우라도 공격자가 두 사용자 사이에 설정된 과거 및 현재의 세션키를 유추할 수 없어야만 한다.

(7) 알려진 키에 대한 안전성(known key security)

키 교환 프로토콜에 참여하는 사용자간에 과거 세션키가 노출되어도 현채 세션키의 안전성에는 어떠한 영향도 미치지 않아야만 한다.

이외에도 사용자의 신원 정보나 거래 정보가 노출되기 쉬운 M-Commerce 환경의 특징을 고려한여 추가적으로 필요한 요구 사항은 다음과 같다.

(8) 이동통신 사용자의 익명성(anonymity of

mobile user)

M-Commerce 호스트가 이동통신 사용자의 신원을 직접적으로 확인하지 못하게 한다.

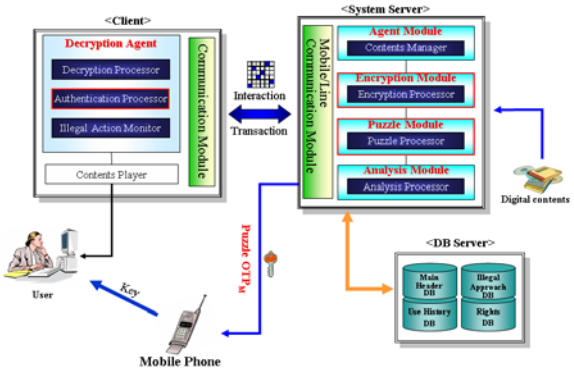
(9) 통신정보의 기밀성(confidentiality)과 무결성(integrity)

키 교환을 하는 두 사용자 사이의 통신내용을 무선통신 사업자를 포함한 제 3자가 알지 못하게 하고, 다른 사람에 의해 통신내용이 변경되지 않음을 보장해야 한다.

3. 제안 시스템 구조

3.1 제안하는 시스템

본 논문에서 제안하는 시스템은 [그림 1]과 같이 클라이언트/서버 구조로 구성되어 운용되고, 서버는 에이전트 모듈과 암호화 모듈, Puzzle 모듈, 분석 모듈과 데이터베이스로 구성되며 클라이언트는 복호화 처리기와 저작물 실행기로 구성된 복호화 에이전트가 있다.



[그림 1] 제안하는 개선된 DRM 시스템 구성도

(가) 서버의 에이전트 모듈

콘텐츠 제공자(CP : Content Provider)에 의해 제공되는 콘텐츠들을 제공받아 등록시켜주는 역할을 제공하며, 등록된 콘텐츠를 서버의 암호화모듈로 전송시켜주는 역할을 한다. 클라이언트의 복호화 모듈에서 들어오는 모든 값들을 수집하여 통계 분석 모듈과 직접 통신하여 정보를 처리 및 관리하는 모듈이다.

(나) 서버의 Puzzle 모듈

디지털 콘텐츠를 사용하고자하는 사용자에게 콘텐츠 암호화키를 Matrix Puzzle 기법으로 암호화하는 역할을 한다. 인증된 사용자에게 Matrix Puzzle과 OTP_M의 조합으로 암호화키를 암호화하고 유선으로 Matrix Puzzle을 무선으로는 OTP_M 값을 전송한다.

(다) 서버의 통계 분석 모듈

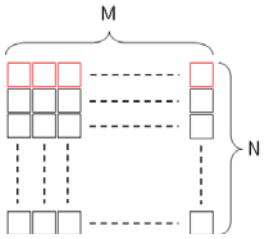
서버에이전트 모듈로부터 받은 클라이언트의 모든 행위에 대한 정보를 감시하고, 데이터베이스 시스템과 연동하여 정보를 얻어내어 분석하는 모듈이다. 처음 접속한 사용자인지 기존 사용자인지를 확인하여 인증번호를 재발급할지 발급된 인증번호를 계속 사용할지를 결정할 수 있는 정보를 제공한다.

(라) 클라이언트의 복호화 에이전트

클라이언트의 복호화 에이전트는 암호화된 컨텐츠를 복호화 하기 위하여 무조건 설치해야 하며, 클라이언트 사용자가 서버에 처음 접속하였을 때 서버로부터 다운로드하여 설치되며 클라이언트 시스템에서 암호화된 콘텐츠를 복호화하여 실행시키기 위해 사용자가 직접 실행시켜야 한다.

3.2 제안하는 시스템 암호화 방법

DRM Server는 [그림 2]와 같이 Matrix Puzzle를 생성하고 암호화 키 길이가 같은 OTP_{T1}과 OTP_{T2}가 들어갈 Matrix Puzzle을 생성한다. 만약 16 * 18의 Puzzle 일 때 행과 열은 0 ~ F까지로 구분한다.



[그림 2] M*N Puzzle

OTP_{T1}과 OTP_{T2}의 생성방법은 기존의 동영상 암호화 키(EK)를 획득한 후 암호화키와 같은 길이의 난수(OTP_{T1})를 생성하고, [식 1]과 같이 암호화키와 OTP_{T1} 을 XOR한 값을 OTP_{T2}로 정의한다.

$EX \oplus OTP_{T1} = OTP_{T2} \Leftrightarrow OTP_{T1} \oplus OTP_{T2} = EK$..[식 1]

3.2.1 OTP_M과 OTP_{T1}생성

Mobile phone으로 전송될 값은 난수 값으로 OTP_M이 생성되며, [그림 3]과 같이 OTP_M값 중에서 처음부터 8번째 문자를 해쉬함수로 수행한 값을 X 좌표, 9번째 문자부터 16번째 문자를 해쉬함수로 수

행한 값을 Y좌표로 구성된다.

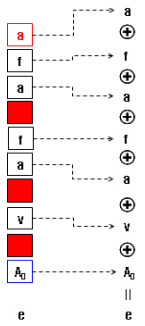
OTP_M = 0123456789ABCDEF
$H(OTP_M)$ = ACFD83723FB6F····193C27D4CEBC90A····
X좌표 (0 ~ F) : A C F D 8 3 7 2 3 F····
Y좌표 (0 ~ F) : 1 9 3 C 2 7 D 4 C E····

[그림 3] OTP_M 값을 해쉬한 후 좌표값 구분

3.2.2 OTP_{T2}생성

OTP_{T2}의 값은 Matrix Puzzle의 마지막 행값의 값이며, [그림 3]에서 언급했던 좌표값(X, Y)을 제외한 값만을 XOR 연산과정을 통해 원래의 암호화 키 EK를 구할 수 있다.

OTP_{T2}의 값은 각 열에서 마킹된 부분을 제외한 나머지를 XOR한 값과 각각의 열에 해당하는 A0 ~ AN까지 값이 OTP_{T2}가 되며 이 값으로 패딩 한다. 이때 OTP_{T2} 값은 “ekapsf5376” 이라 가정하고 OTP_{T2}의 자세한 생성 방법은 [그림 4]와 같다.



[그림 4] OTP_{T2} 값 생성 방법

연산으로 A_0 이전의 값과 A_0값을 XOR하면 [그림 4]와 같이 e(OTP_{T2})값이 나오고, A_0의 값을 구한다. A_0의 값을 패딩 하여 OTP_{T1}과 OTP_{T2} 값을 Matrix Puzzle에 넣어서 전송하므로 해커로부터 암호화 키 유추가 불가능하고, OTP_{T2}값을 얻는 방법은 [식 2]와 같다.

$$a \oplus f \oplus a \oplus f \oplus a \oplus v \oplus A_0 = e \quad \text{.....[식 2]}$$

3.3 제안하는 시스템 복호화 방법

Puzzle 복호화는 DRM Server로부터 다운 받은 콘텐츠와 Puzzle, OTP_M를 이용하여 복호화 한다. 복호화 과정은 암호화 기법의 역순으로 진행된다.

복호화 과정을 보면 먼저 Mobile phone으로 전송 받은 OTP_M값을 해쉬함수를 수행한다.

에이전트로부터 전송받은 퍼즐과 $H(OTP_M)$값을 이용하여 Puzzle에 숨겨진 두 개의 키를 획득한다. 이렇게 Puzzle로부터 획득한 두 개의 키를 XOR하여 암호화 키를 획득 할 수 있다. 이렇게 획득된 암호화키로 디지털 콘텐츠를 재생 시킨다.

4. 실험평가

4.1 안전성에 대한 평가

안정성에 대한 평가는 매트릭스 Puzzle을 유선망으로 DRM 서버에서 클라이언트로 보내줄 때 매트릭스 Puzzle에 대한 암호화 키 유추 가능한 방법에 대해서 서술한다.

스니핑 공격 : SSL 채널을 통해 유선망으로 Puzzle을 전송하며 또한 공격자가 만약 Puzzle을 획득할 수가 있다 하더라도, 무선망의 Puzzle 홀값을 유추하지 못하기 때문에 스니핑 공격에 대해 안전하며, 또한 유선망 또한 새로운 키를 전송할 때마다 항상 다른 Puzzle을 전송하기 때문에 스니핑 공격에 안전하며, SSL 채널은 아직까지는 안전하기 때문이다.

스푸핑 및 재전송 공격 : 모바일폰을 이용하여 사용자를 인증하기 때문에 무선망의 Puzzle 홀값을 유추하지 못한다. 또한 Puzzle 홀값을 유추할 때 사용한 해쉬 알고리즘 역시 알 수가 없기 때문에 스푸핑 및 재전송 공격에 대해 안전하다. 다음과 같은 가정은 모바일폰은 유선에서 알 수 없다는 가정이고, 비록 알아냈다고 하더라도 SSL 채널상의 매트릭스 Puzzle을 알아낼 수가 없기 때문이다.

4.2 암·복호화에 대한 실험평가

기존 DRM 시스템은 인증서를 사용하는 경우 인증서 확인 작업 및 키를 암호화 복호화 하는데 많은 오버헤드가 발생하며, 인증서 미소지시에는 인증서 발행하기 위한 절차가 많이 까다롭다. 그러나 인증서를 사용한 공개키 암호화 방식은 어떠한 공격에 대해서도 안전하다는 장점이 있다. 인증서를 사용하지 않는 DRM 시스템의 경우는 콘텐츠를 보호하는 암호화키를 대칭키로 사용하여 전송하기 때문에 서로간의 키 교환 문제가 어려우며, 유선망을 사용하기 때문에 스니핑 공격에 대해 취약하다.

제안한 DRM 시스템은 암호화키를 전송하기 위해 Puzzle을 생성한 후, 연산속도가 빠른 XOR만을 사용하여 해당 Puzzle을 복호화하기 때문에 속도가 매

우 빠르며, 무선망을 이용하여 좌표값을 생성하는 키를 따로 전송하기 때문에 키 조합으로 인한 키 유추가 매우 어렵다. 또한 Puzzle 자체에는 어떠한 암호화도 되어있지 않아 바로 실행이 가능하며, 키 요청마다 새로운 Puzzle을 전송하기 때문에 스니핑, 스푸핑, 재전송 공격에 강한 특징을 가진다. 사용자 키 입력 횟수는 별다른 암호화를 사용하지 않기 때문에 모바일로부터 입력받은 키만 입력하면 복호화 과정까지 전부 자동으로 진행되기 때문에 로그인 시점의 키 입력까지 합쳐 모두 2번의 입력으로 가능하다.

5. 결론

인터넷의 확산과 컴퓨터 간 상호연결성의 증대로 디지털 자원에 대한 유통환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 멀티미디어 자료에 대한 수요가 급격히 증가로 인해 불법복제 방지를 위한 디지털 저작권 보호문제가 중요한 이슈로 대두되고 있다.

기존의 DRM 시스템은 하나의 대칭키로 암호화하는 것이므로 사용자가 해당 대칭키를 노출시키면 더 이상 해당 저작물에 대한 보호를 보장받지 못하며, 또한 키를 노출시킨 사용자가 누구인지 알 수 없어서 해당 사용자를 추적할 수 있는 방법이 없다.

기존의 One-path XOR 방식은 비트값이 전부 1일 경우 기존의 키가 나오는 단점과 유·무선으로 전송되는 각각의 값의 결합으로 암호화키가 나온다는 단점도 있다. 그러나 제안하는 방식은 유선의 Matrix Puzzle과 무선의 모바일키를 이용하여 연산속도가 빠른 XOR 만을 수행한 후 암호화키를 획득한다. 유선의 Matrix Puzzle은 어떠한 암호화도 시키지 않았기 때문에 암호화키 유추시 수행시간을 향상 시켰으며 Matrix Puzzle이 유추 되더라도 무선으로 보내지는 OTPM값없이는 암호화키(EK)의 유추가 불가능하다. 또한 키 요청마다 새로운 Puzzle을 전송하기 때문에 기존 시스템보다 스니핑, 스푸핑, 재전송 공격에 강한 특징을 가지고 있으며, 사용자 키 입력 횟수는 별다른 암호화를 사용하지 않기 때문에 모바일로부터 입력받은 키만 입력하면 복호화 과정까지 전부 자동으로 진행되기 때문에 로그인 시점의 키 입력까지 합쳐 모두 2번의 입력으로 가능하다.

향후 연구과제로는 연산 수행능력이 현저히 떨어지는 휴대용 기기 및 Off-line 상에서 사용할 수 있는 방법과 기존 시스템 중 콘텐츠 암호화 기법을 연구한 논문과 제안된 키 교환 방법을 결합하여 더욱 우수한 DRM 시스템을 연구할 것이다.

참고문헌

[1] 정용훈 “멀티미디어 콘텐츠 보호를 위한 인증 프로토콜에 관한 연구 ,” 숭실대학교 석사학위논문, 2006.

[2] 추연수, “디지털 콘텐츠 보호를 위한 안전한 인증 방식 설계 및 구현,” 숭실대학교 석사학위논문, 2005.

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

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

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

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

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

[8] Shai Halevi, Hugo Krawczyk, "public-key cryptography and password protocols," ACM Transactions on Information and System Security, Vol.2, No3, August 1999, pp230-268

[9] Thomas Wu. "The Secure Remote Password Protocol," 1998 Internet Society Network and Distributed System Security Symposium, San Diego, March 1998, pp97-98 .