PKI 기반의 라이선스 에이전트를 이용한 암호화 기법 관한 연구

고재운
콤넥스시스템
e-mail:gjwmr@naver.com

A Study of Protection Mechanism using License Agent based PKI

Jae-Woon Ko
Comnex System Inc.

요 약

본 논문에서는 동영상 데이터 암호화를 위해 비디오 데이터의 I-프레임 암호화 기법을 제안한다. 또한 시스템 서버에서 암호화된 멀티미디어 데이터를 클라이언트 시스템에서 사용자가 실행할 때 자동으로 사용자 인증과 데이터의 복호화를 수행할 수 있도록 하는 라이선스 에이전트를 제안한다. 라이선스 에이전트는 사용자의 멀티미디어 데이터의 실행 시 공유 키 풀(shared key pool)을 이용한 PKI(Public Key Infrastructure)기반의 사용자의 인증과 멀티미디어 데이터의 암호 및 복호화를 수행한다. 또한 비밀키 기반의 공개키 분배 시스템을 이용하여 키의 누출을 미연에 방지하고 키의 누출 시 그 경로를 추적할 수 있도록 하였다.

1. 서론

최근 DRM(Digital Rights Management) 기술을 통해 디지털 저작물에 대한 지적재산권 침해사례로부터 저작권을 보호하고, 유통과정을 관리하기 위한 종합적인 대책이 추진되어 저작물에 대한 제작, 유통, 이용 등이 일련의 신뢰할 수 있는 환경에서 이루어질 수 있도록 하는 다양한 연구가 진행 중에 있다[1. 2]. 기존의 DRM은 사용자의 프라이버시 보호가 저작권 보호에 직접적으로 필요하지 않는다는 이유로 사용자의 프라이버시 보호에 대해서는 고려하지 않았다. 이러한 영향으로 라이센스 발급시의 사용자 인증과 컨텐츠의 불법 사용 감시를 위한 사용내역 보고 과정에서 사용자 정보가 유출되는 문제점이 발생하였고, 이로 인해 사용자 프라이버시 침해 문제가 발생하게 되었다[3, 4].

디지털 저작물에 대한 보안을 처리하기 위한 방식으로는 상위레벨에 대한 보안과 하위레벨에 대한 보안의 두 가지로 나눌 수 있다[5]. 상위 레벨의 보안 방식은 사용자에 대한 인증이고 하위레벨에 대한 보안은 데이터 자체에 대한 보호이다. 사용자에 대한 인증이란 인증을 받은 사용자는 저작물을 아무런 제약없이 사용할 수 있는 것으로서 저작물 사용에 제약을 받지 않는 것이다[6]. 그러므로 사용자가 어떤 저작물을 몇 번 사용했는지에 대한 정보를 유지하기 위한 저작물 사용량 감시기능이 반드시 필요하다[7]. 그러나 이 보안 방식은 인증된 사용자가 데이터를 불법 복제하여 유통할 수 있기 때문에 유통되는 데이터를 완전히 보호할 수 없는 단점이 존재한다. 이에 반하여 데이터 자체에 대한 보호는 저작물 자체에 암호화를 수행하여 저작물에 대한 사용자의 접근을 제한하는 방식이다. 그러므로 DRM에서 보안기술로는 데이터 자체에 대하여 암호화를 수행하는 보안 방식을 사용한다.

본 논문에서는 디지털 콘텐츠 사용자 인증에 있어서 사용자에 의한 비밀키의 노출을 막기 위하여 비밀키를 각 사용자별 개인정보를 이용하여 암호화하는 공유 키 풀 기법을 제안하여 사용자에 의한 비밀키의 노출을 막으면서 동시에 저작물을 미리 암호화하여 전송 속도를 개선한 새로운 기법을 제안하였다. 또한 라이선스 에이전트를 이용하여 저작물 실행 시 라이선스 서버로부터 라이선스를 다운로드 받아서 자체적으로 데이터베이스에 관리하여 오프라인에서도 실행이 가능하도록 하였다.

2. 관련연구

DRM 기술을 이용하여 InterTrust사와 Microsoft 사 등의 외국 업체와 Digicap와 같은 국내 여러 업체가 다양한 형태의 DRM 솔루션을 제공하고 있다[8]. 그러나 기존 DRM 솔루션들은 암호화에 사용하는 키로 비밀키를 사용하여 사용자가 파일을 다운로드할 때 암호화를 수행하므로 많은 시간이 소요된다. 또한 복호화를 수행하는 경우에도 대용량의 저작물인 경우 전체 파일에 대하여 복호화를 먼저 수행한 후에 실행을 할 수 있으므로 사용자가 실시간으로 파일을 실행할 수 없는 문제점이 존재한다. 또한 암호화와 복호화에 사용하는 키가 사용자에 의하여 노출이 된다면 해당 저작물에 대한 보호는 더 이상 보장하지 못하는 단점이 있다. 그리고 기존의 DRM 솔루션들은 동영상 데이터 안에 데이터의 보호조건이나 저작관리 등의 정보를 삽입하여 관리를 수행하는 정적인 저작권 관리를 하기 때문에 저작권에 대한 동적인 제어가 어려울 뿐 아니라, 감시 및 추적 기능의 제약으로 불법적인 복제 등 지적재산권 침해 발생 시 불법행위 입증에 필요한 자료 확보의 어려움 등 해결해야 할 많은 과제를 가지고 있다. 그러므로 기존의 DRM은 이 문제를 해결하기 위해서 소프트웨어 에이전트를 사용하여 사용자의 데이터 사용을 모니터링 하기도 하지만 오프라인 환경인 경우 그 기능상에 많은 제약을 가지고 있다. 따라서 온라인 및 오프라인 환경에서 모든 저작물 유형에 적용이 가능하면서 동적인 저작권 관리와 실시간 감시 및 추적을 가능하게 하는 디지털저작권관리 기술의 개발이 필요한 실정이다.

3. 암호화 기법

원 저작물의 데이터 보호와 인증을 위해 기존의 저작물에 대한 단순한 사용권한 제한이나 패스워드 인증 방식이 아닌 PKI 기법을 이용한 사용자 인증과 데이터 암호화를 이용하여 원 저작물에 삽입하여 데이터를 보호해야 한다.

저작물 저작자는 창작한 저작물을 서버에게 전송한다. 그러면 서버는 해당 저작물을 임의의 비밀키 Ks로 암호화하여 암호화된 저작물 C를 서버의 저작물 데이터베이스에 비밀키 Ks와 같이 저장한다.

$$C=EKs[data] \quad (1)$$

공유 키 풀(Shared Key-Pool)을 구성하기 위해서 저작물 제작자는 분배할 동영상을 비밀키 Ks를 사용하여 암호화하며 식 2와 같이 k개의 비트열로 나눌 수 있다.

$$Ks = Ks_1 | Ks_2 | \cdots | Ks_k \quad (2)$$

일반적으로 비밀키 암호화에서 비밀키 Ks는 128 비트를 사용한다. 암호화에 사용한 비밀키의 보안성을 높이기 위해서 비밀키를 공유 키 풀을 사용하여 암호화 한다. 공유 키 풀은 $k * 2^{\frac{n}{k}}$개의 비트로 구성되며 식 3과 같이 생성한다.

$$\left\{a_1^0, a_1^1, a_1^2, \cdots, a_1^{2^{\frac{n}{k}-1}}, a_2^0, a_2^1, a_2^2, \cdots, a_2^{2^{\frac{n}{k}-1}}\right\} \left\{, \cdots, a_k^0, a_k^1, a_k^2, \cdots, a_k^{2^{\frac{n}{k}-1}}\right\} \quad (3)$$

각 사용자에 대한 개인용 키 Kp는 k비트로 이루어진 식 4와 같은 비트열의 집합이다.

$$Kp = a_1^{b_1} | a_2^{b_2} | \cdots | a_k^{b_k} \quad (4)$$

이 때 b_i는 식 5와 같으며 키 풀에서 각 i 번째 행의 값으로서 사용자의 개인용 키를 결정하는 중요한 값이다. b_i는 사용자 인증서의 공개키에서 추출한다.

$$B = b_1 | b_2 | \cdots\cdots | b_k \quad (5)$$

사용자의 공개키는 일반적으로 비도가 낮은 경우에는 512비트의 값을 사용하고 비도가 큰 중요한 정보인 경우에는 1024비트의 값을 사용한다. 일반적으로 n비트의 공개키를 사용하는 경우 개인용 키의 길이가 k비트라면 이 때 키 풀의 각 항목의 값은 $2^{\frac{n}{k}}$ ($0 \sim 2^{\frac{n}{k}}-1$)의 값의 범위를 가지게 된다. 예를 들어, 공개키의 길이가 512비트이면서 개인용 키의 길이가 128비트라면 512/128=4이므로 각 항목의 값은 24=16이 되어 16진수로 0~F의 값을 가지게 된다. 그러므로 공개키의 값 0~F에 따라서 실제 개인용 키의 각 행이 결정되게 된다.

그러므로 각 사용자들의 개인용 키는 자신들의 유일

한 공개키 값에 의해서 결정되므로 공개키에 의해서 각 행에서 선택된 키 값은 모든 사용자에게 다른 키가 배정되는 것을 보장해준다. 공유 키 풀이 생성되면 비밀키 Ks를 암호화하기 위하여 공유 키 풀의 각 i번째 행에 대하여 $2^{\frac{n}{k}}$개의 비트인 $a_i^0, a_i^1, \cdots, a_i^{2^{\frac{n}{k}-1}}$에 각각 Ks_i와 비트 단위의 배타적 논리합(bit-wise XOR)을 하여 식 6과 같이 구한다.

$$a'^0_i = Ks_i \oplus a^0_i, \quad a'^1_i = Ks_i \oplus a^1_i, \quad \cdots\cdots, \quad a'^F_i = Ks_i \oplus a^F_i \qquad (6)$$

암호화된 공유 키 풀은 이제 네트워크를 통하여 사용자 에이전트에게 전달된다. 에이전트는 암호화된 동영상 파일을 복호화하기 위하여 암호화된 키 풀에서 사용자의 비밀키 Kp를 이용하여 비밀키 Ks를 찾아낸다. 이 비밀키 Ks를 이용하여 동영상 파일을 복호화하여 사용자에게 보여준다. 에이전트가 암호화된 키 풀과 개인용 키 Kp를 가지고 비밀키 Ks를 찾는 방법은 식 7과 같다.

$$\text{Kp} = a^{b_1}_1 | a^{b_2}_2 | \cdots | a^{b_k}_k \text{ 이고 } a'^j_i = Ks_i \oplus a^j_i$$

이므로

$$a^{b_1}_1 \oplus a'^{b_1}_1 = a^{b_1}_1 \oplus Ks_i \oplus a^{b_1}_1 = Ks_i \qquad (7)$$

예를 들어, n=4, k=4인 경우 b는 $2^{\frac{4}{4}} = 2^1 = 2$가 되어 {0~1}의 값을 갖는다.
b = {0, 0, 1, 0}이라고 하면 사용자의 개인키는 { $a^0_1, a^0_2, a^1_3, a^0_4$ }= {1, 0, 0, 1} 이 된다. 비밀키가 Ks = {1, 1, 1, 0}이라고 하면 암호화된 키 풀은 비밀키 Ks_i와 비트 단위의 배타적 논리합(bit-wise XOR)을 하여 식 8과 같이 구할 수 있다.

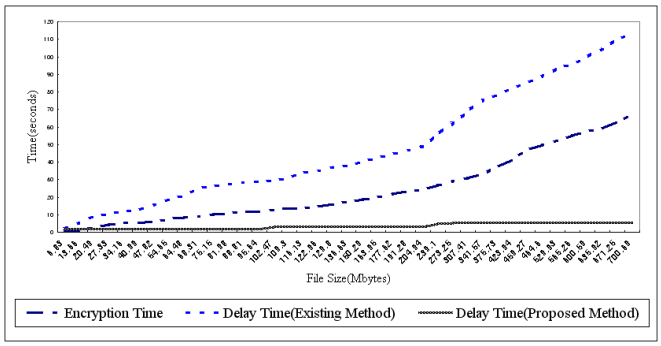
{1, 1, 1, 0} ⊕ {1, 0, 0, 1} ={0, 1, 1, 1}
{1, 1, 1, 0} ⊕ {1, 1, 0, 1} ={0, 0, 1, 1} (8)

사용자 에이전트는 암호화된 키 풀과 개인키를 이용하여 비밀키 Ks를 식 9와 같이 구할 수 있다.

{1, 0, 0, 1} ⊕ {0, 1, 1, 1} ={1, 1, 1, 0} (9)

4. 성능평가

본 논문에서 제안하는 기법과 알고리즘에 의해 복호화를 수행하면서 이중 버퍼 스케줄링에 의해 동시에 비디오 데이터 파일을 재생하므로 기존의 기법보다 현저하게 재생 지연시간이 감소하였음을 확인할 수 있다. 그림 1은 39개의 비디오 데이터를 이용하여 기존기법과 제안하는 기법의 암호화 시간과 재생 지연시간을 측정한 후 그래프로 나타내었다.



[Fig. 1] Encryption Time and Delay Time Comparison.

기존의 기법은 동영상의 크기에 비례하여 암호화 시간이 늘어나며 지연시간 역시 비례하여 늘어나는 것을 알 수 있다. 그러므로 기존의 기법을 대용량의 동영상 데이터에 사용할 경우 많은 지연시간이 발생하여 사용자에 대한 서비스 지연 시간이 늘어나게 된다. 이에 반하여 제안하는 기법은 동영상의 크기에 비례하여 암호화 시간이 늘어나지만 복호화를 수행하면서 동시에 재생을 하므로 로딩 시간이 줄어들어 실제 지연시간은 줄어드는 것을 알 수 있다.

5. 결론

본 논문에서는 동영상 데이터 암호화를 위해 비디오 데이터의 I-프레임을 암호화하는 새로운 암호화 기법을 제안하였다. 또한, 시스템 서버에서 암호화된 멀티미디어 데이터를 클라이언트 시스템에서 사용자가 실행할 때 자동으로 사용자 인증과 데이터의 복호화를 수행할 수 있도록 하는 라이선스 에이전트를 제안하였다. 라이선스 에이전트는 사용자의 멀티미디어 데이터의 실행 시 공유 키 풀을 이용한 PKI 기반의 사용자의 인증과 동영상 데이터의 암호 및 복호화를 수행한다. 비밀키를 사용하여 동영상 파일을 암호화한 후, PKI 인증서와 공유 키 풀과의 연산을 통하여 사용자의 개인정보를 추출하고 비밀

키를 공유 키 풀에 감추어서 사용자에게 전송하여 사용자가 비밀키에 접근하여 키를 외부에 노출시키는 것을 원천적으로 방지하였으며 키의 누출 시 그 경로를 추적할 수 있도록 하였다. 공유 키 풀 시스템은 사용자에 의한 키의 노출에 효과적으로 대응할 수 있는 기법이다.

제안하는 시스템은 동영상에 대한 DRM 시스템으로서 인터넷을 통한 영화 및 뮤직비디오, CF 등의 동영상 서비스의 저작권 보호에 사용된다면 좋은 효과를 기대할 수 있다.

참고문헌

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

[2]Jai Sundar B., Spafford E., "Software Agents for Intrusion Detection," Technical Report, Department of Computer Science, Purdue University, 1997.

[3]J.Dubl,"Digital Rights Management: A Defination", IDC 2001.

[4]J.Dubl, S.Kevorkian, "Understanding DRM system: An IDC White paper", IDC, 2001.

[5]Kentaro Endo, “The Building up of national Regional and International Registers for works and objects of related rights," Proc. of International Conference on WIPO, Seoul, Korea October 25-27, 2000.

[6]V. K Gupta, "Technological measures of protection," Proc. of International Conference on WIPO, Seoul, Korea October 28-29, 2000.

[7]P. Vora, D, Reynolds, L. Dickinson, J. Erickson, D. Banks, "Privacy and Digital Rights Managements", A Position paper for the W3C Workshop on Digital Rights Management, January 2001.