DRM 시스템을 위한 안전한 복호화 키 분배 시스템 설계

추연수° 이영구 전문석
숭실대학교 일반대학원
{lets-priase, ad3927}@hanmail.net°

Design Secure Key of Decryption Distribution System for DRM System

Yeoun-Soo Choo°, Young-Gu Lee, Moon-Seog Jun
Soong-Sil University

요 약

PC 사용의 증가로 많은 아이템들이 디지털화 되어 사용되고 있다. 복제되어도 그 질이 떨어지지 않는다는 특성을 디지털 콘텐츠는 불법적으로 복제되어 사용, 유포되고 있다. 이로 인해 많은 콘텐츠 제공자들은 지적 재산권의 피해를 보고 있어서 DRM 기술이 연구, 개발되고 있다. DRM 기술은 콘텐츠를 암호화하여 허가된 사용자들에게만 사용권을 주는 기술인데 이 기술을 적용하기 위해서 암호화 키의 분배가 필수적이다. 기존의 DRM 시스템은 PKI를 적용하여 키 분배를 하고 있는데 PKI를 적용하면 키 분배를 위해서 복잡한 사전 작업이 필요하고 처리시간도 만만치 않다. 본 논문에서는 모바일 폰을 이용한 복호화 키 분배 시스템을 설계한다.

1. 서 론

현대 사회에서 PC는 간단한 문서 작업뿐만 아니라 쇼핑과 재테크 업무에 이르기까지 다양한 역할을 감당하고 있다. 또한 e-book을 통한 독서나, 음악, 영화감상은 아이템들이 디지털화 되어 보급, 서비스 되고 있다. 디지털 콘텐츠의 특성상 복제하여 원본과 동일한 컨텐츠를 얻을 수 있다. 이 특성을 악용하여 지식을 기반의 컨텐츠들이 무분별하게 불법적으로 유포되고 있어서 제작자들의 권리가 침해당하고 있다. 이러한 문제를 해결하기 위해서 DRM(Digital Right Management)기술이 연구되고 있으며 실제로 이 기술을 이용한 솔루션들이 출시되어 제작자들의 권리를 보호하고 있다. 이 DRM 시스템은 컨텐츠를 보호하기 위해서 암호 알고리즘을 사용하여 컨텐츠를 암호화 하고 정당한 사용자들에게는 암호화된 컨텐츠를 복호화 할 수 있는 키를 전달함으로써 컨텐츠를 사용할 수 있게 하고 있다. 키를 전달함에 있어서 기존의 DRM 시스템들은 공개키 기반 구조를 사용하고 있다. 이 방법은 사용자와 서비스를 제공하는 제공자가 미리 자신들의 인증을 위해서 처리해야하는 전처리 과정이 있어야 하는 다소 복잡하다는 문제와 이 처리과정을 거치면서 발생하는 지연시간이 문제점으로 남아 있었다.

본 논문에서는 이 문제점을 해결하기 위하여서 사용자의 모바일 폰을 이용한 새로운 키 분배 방식을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 컨텐츠를 암호화 하는데 사용되는 암호화 기술과 저작권 보호 기술에 대해 기술한다. 3장에서는 제안하는 키 분배 방식을 제안하고 4장에서는 결론과 향후 연구방향을 제시한다.

2. 관련연구

2.1 암호화 기술

암호 기술의 기원은 전쟁의 역사에서 찾아 볼 수 있다.

기원전 450년경, 그리스의 도시국가 스파르타에서 파견된 첩자는 동맹국 페르시아의 배신을 감지하고 이를 암호화하여 자국에 알렸는데 이것이 암호 기술의 기원이다.[1] 암호 기술에는 암호화에 사용되는 키의 개수에 따라 암호화를 위한 키와 복호화를 위한 키가 서로 다른 공개키 암호기술과 암, 복호화를 위한 키가 한 개뿐인 비공개키 암호기술이 있다. 공개키 암호기술은 PKI라는 큰 인프라에 속에서 사용되며 개인 인증과 증명을 위해서 주로 사용된다. 비공개키 암호 기술은 다시 블록 암호 알고리즘과 스트림 암호 알고리즘으로 나뉘는데 블록 암호 알고리즘은 평문을 일정한 블록 단위로 나누어 암호화를 실행하는 알고리즘으로 DES, AES가 대표적인 알고리즘이고, 스트림 암호 알고리즘은 평문을 나누지 않고 1비트 단위로 암호화를 실행하는 알고리즘이다. 대표적인 알고리즘으로는 RC4, SEAL이 있다.

2.2 저작권 보호 기술

PC 사용의 증가로 인터넷의 사용이 증가하게 되었고 지식 기반의 아이템(e-book, mp3, 동영상화일)들이 디지털화 되어 많은 사용자들에게 제공되면서 디지털 컨텐츠 제작자들의 권리 보호 문제가 대두되었다. 디지털 컨텐츠는 복제가 쉽고 복제되어도 그 질이 떨어지지 않는다는 특성을 가지고 있다. 이 특성을 이용한 불법적인 유통과 사용을 막기 위해서 저작권 보호 기술이 연구, 개발되고 있다. 현재 외국 기업으로는 InterTrust사와 Microsoft사 등이 있고 국내 기업으로는 디지캡과 마크애니 등이 DRM(Digital Right Management)솔루션을 출시하고 있다. DRM 시스템은 비즈니스 룰을 통하여 컨텐츠에 대한 대가를 지불한 사용자들에게 서비스를 해주는 시스템을 말한다.

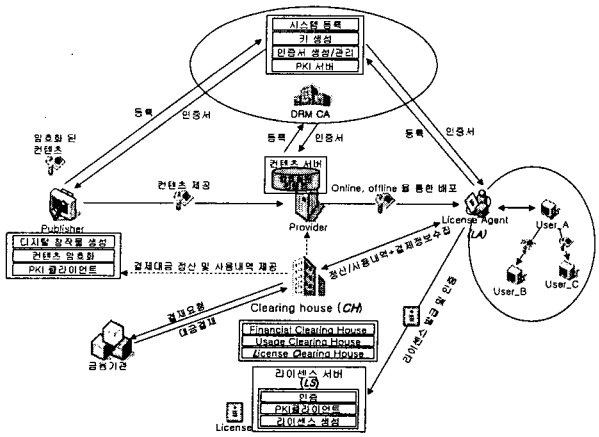

그림 1 DRM 시스템 구성도

DRM 시스템은 그림 1 과 같이 일반적으로 컨텐츠를 사용하는 사용자, 컨텐츠를 가공하고 서비스를 해주는 DRM 서버와 사용자와 사이트를 인증해주는 인증기관, 초기 컨텐츠를 제작, 제공하는 제공자, 라이선스를 제공하는 라이선스 서버, 과금에 대한 처리를 하는 클리어링하우스로 구성되어진다. DRM 시스템은 이 구성원들이 유기적인 관계를 유지하면서 대가를 지불한 정당한 사용자에게 컨텐츠를 서비스하게 된다.

2.2.1 키 분배 기술

DRM 시스템은 정당한 사용자 외에는 컨텐츠에 대한 사용을 제한하기 위하여 컨텐츠에 대한 가공, 즉 암호화를 미리 수행하여 컨텐츠를 보관하고 정당한 사용자의 요청이 있을 때 컨텐츠와 복호화를 위한 키를 전송해 줌으로써 컨텐츠를 서비스한다. 때문에 이 키 분배를 어떻게 하느냐가 DRM 서비스의 성공과 실패를 가늠할 수 있는 중요한 요소가 된다.

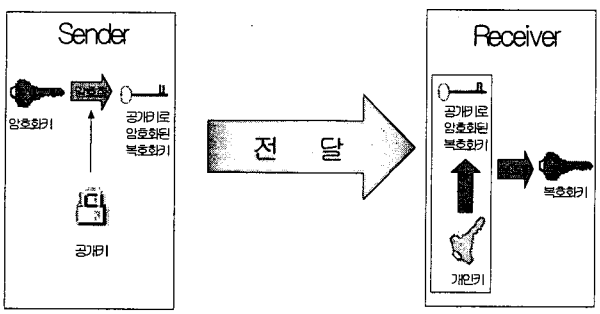

그림 2 DRM 시스템에 적용된 기존의 키 분배 방식

기존의 키 분배 방식은 그림 2 과 같이 상대적으로 암호화 속도가 빠른 비공개키 알고리즘을 이용하여 컨텐츠를 암호화한 후 복호화 키를 수신자의 공개키로 암호화하여 수신자에게로 전송하였다. 수신자의 공개키로 암호화 된 메시지는 수신자의 개인키로만 복호화할 수 있기 때문에 수신자는 안전하게 복호화 키를 전송 받을 수 있었다. 하지만 DRM 서버가 수신자의 공개키를 사용하기 위해선 PKI를 이용한 인증 시스템이 마련되어 있어야 하고 또한 DRM 서버가 획득한 공개키가 수신자의 공개키가 맞는 지에 대한 사전 검증 작업도 필요하다. 또한 사용자가 컨텐츠를 사용하기 위해 접속하는 사이트가 합법적으로 컨텐츠를 서비스하는 사이트인지를 검증이 필요하다. 이런 사전 작업이 많이 필요하고 인증서 사용의 복잡성 때문에 인증 처리 시간이 오래 걸린다는 단점이 있다.

3. 제안하는 키 분배 시스템

본 논문에서 제안하는 키 분배 시스템은 기존의 키 분배 방식에서 사용되었던 공개키 기반 구조를 사용하여서 발생하는 처리 시간 지연과 사용자가 사전에 처리해야하는 복잡한 인증서 획득 문제를 공개키 기반 구조를 사용하지 않음으로 해서 해결하였다. 또한 누구나 사용하고 있는 모바일 폰을 이용하여서 인증서를 통한 인증방식의 처리 지연과 복잡성을 해결하였다.

3.1 키 분배 방식

제안하는 키 분배 방식은 DRM 서버와 사용자가 사이트에 접속할 때 사용자의 PC에 설치되는 Agent를 통하여 키 분배가 이루어진다. 제안하는 키 분배 방식은 그림 3 과 같다. 서버에서 사용자 인증과 라이선스에 대한 분석이 끝나면 서버는 해쉬 함수를 통해 일정한 비트열의 분할키_1(Key_S-1)을 만들어 낸다. 서버에 저장되어 있는 암호화키(Key_C)와 XOR 연산을 하여 분할키_2(Key_S-2)를 생성한다. 서버는 Key_S-1는 사용자의 모바일 디바이스로 Key_S-2는 인터넷을 통한 사용자의 Agent로 전송한다. 사용자가 컨텐츠를 실행하려할 때 Agent는 사용자에게 Key_S-1를 요청하고 사용자는 키보드 펀칭을 통해 Key_S-1를 제공한다.

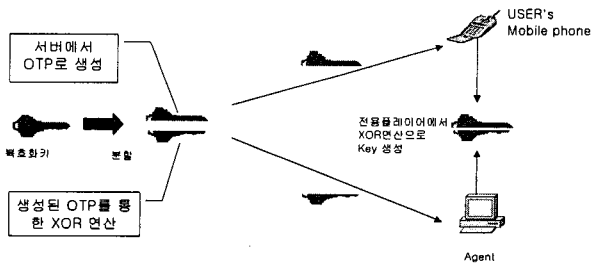

그림 3 제안하는 키 분배 방식

Agent는 제공받은 Key_S-1와 서버로부터 전송받아 저장하고 있는 Key_S-2를 XOR 연산하여 Key_C를 생성하여 사용자가 요구한 컨텐츠를 실행시킨다. 컨텐츠 실행을 위해 사용된 키는 사용된 후 폐기되도록 Agent가 설계되어

져 있다. 서버에서 Key_S-1을 위해 실행되는 해쉬함수는 매번 다른 결과값을 생성하도록 설계되어 사용자와 Agent가 받는 분할키는 매번 다르다. 그러므로 인터넷이나 사용자의 모바일 디바이스로 전송되는 분할키는 공격자에게 가로채여도 안전하다.

3.2 Server 와 Agent

제안하는 키 분배 시스템은 DRM 서버와 Agent를 통하여서 모든 과정이 이루어진다. Server와 Agent의 내부 구조는 그림 4 와 같다. 서버는 컨텐츠 암호화를 위한 암호화 모듈, 분할키와 인증키 생성을 위한 OTP(One Time Password)생성 모듈, 분할키 연산과 사용자 인증을 위한 해쉬함수 연산을 위한 연산 비교 모듈, 복호화키를 분할하기 위한 키 분할 모듈 등이 주를 이룬다. Agent는 개인인증과 사용자 PC인증에 필요한 하드웨어 정보 수집을 위한 하드웨어 정보 수집 모듈, 인증키와 분할키의 사용자 입력을 위한 이벤트 생성 모듈, 복호화키 연산과 인증을 위한 해쉬 함수 연산을 위한 연산 모듈, 복호화된 컨텐츠 실행을 위한 컨텐츠 실행기로 구성되어 있다.

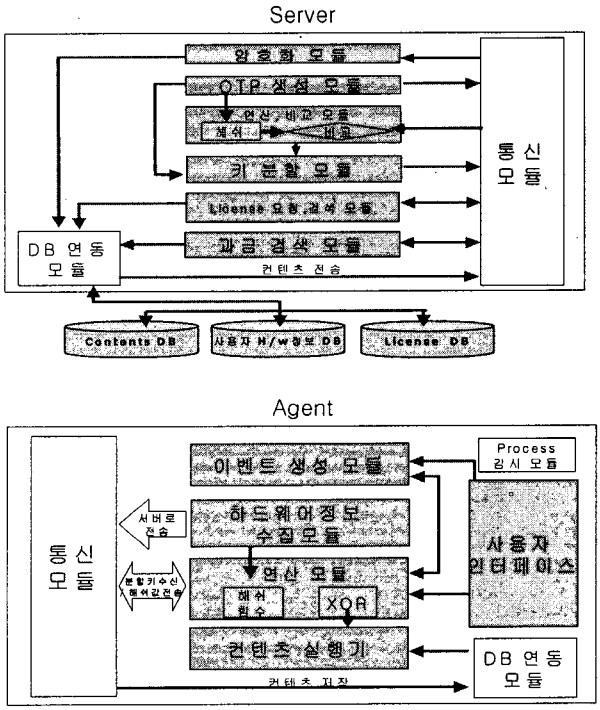

그림 4 Server와 Agent 구조

사용자가 사이트에 접속할 때 사용자 PC에 설치되는 Agent가 서버와 통신하여 분할키를 전송하기 때문에 전처리 과정을 거치지 않는다. 또한 PKI를 사용하지 않기 때문에 복호화키를 전송하는데 있어서 공개키로 암호화하는 암호화 과정이 불필요하다. 때문에 기존의 키 분배 방식에서 문제시 되었던 처리 시간과 복잡한 처리과정을 생략할 수 있으며 간단한 XOR 연산을 통하여서 키 분할 생성을 할 수 있기 때문에 처리 시간에서 기존의 DRM 시스템 보다 월등해진다.

4. 결론

본 논문에서는 기존의 PKI를 이용한 복호화키 분배 시스템에 대한 처리 지연 시간과 복잡성을 해결하기 위해서 현대인이 대부분 소지하고 있는 모바일 폰을 이용하여 키 분배 시스템을 제안하였다. PKI를 이용한 키 분배 시스템은 안정성 면에서 좋은 성능을 가지고 있지만, PKI를 적용하기 위한 전처리 과정의 복잡성과 이 복잡한 전처리 과정을 처리하는데 처리 지연 시간의 문제점을 가지고 있다. 본 논문에서 제시한 키 분배 시스템은 기존의 시스템에서 가지고 있던 문제점을 해결할 수 있을 것이다. 하지만 본 제안 시스템은 개인이 한 대의 모바일 폰을 소지하고 있는 환경을 가정한 것이고 모바일 폰으로 보내지는 SMS 메시지에 대해서는 안전하다고 가정한 것이다. 사용자의 모바일 폰으로 보내지는 메시지에 대한 보안성에 대해서 향후 연구 되어져야 할 것이다.

참고문헌

[1] H.X.MEL 외, 보안과 암호의 모든 것, 인포북, 2001

[2] 우연옥, 황성철, 강홍식, "IPSec에서의 보안강화를 위한 키 프로토콜 연구", 한국정보처리학회 추계학술발표대회 10권 2호, 2003

[3] 김지홍, 이만영, 류재철 송유진, 염흥렬, 이임영 전자상거래 보안 기술, 생능출판사, 2001

[4] 전문석 외, 정보이론 및 PKI, 미래컴, 2003

[5] IETF, RFC2289 A One-Time Password System 1998

[6] IETF RFC2409 The Internet Key Exchange(IKE) 1998