SSL을 이용한 암호 및 인증 서버/클라이언트의 구현

박영민 °, 강민섭
안양대학교 컴퓨터공학과
mskang@aycc.anyang.ac.kr

Implementation of Encryption and Authentication Server/Client Using SSL Protocol

Young-Min Park°, Min-Sup Kang
Dept. of Computer Engineering, Anyang University

요 약

DRM(Digital Rights Management)은 디지털 컨텐츠의 저작권자 권리를 보호하고 인터넷상에서 안전한 거래를 보장하는 기술이다. DRM 기술에 있어서 암호 및 인증을 위한 서버 및 클라이언트 설계는 중요한 부분을 차지하며, SSL(Secure Socket Layer)은 높은 안정성으로 인하여 네트워크 통신을 위한 프로토콜로 가장 많이 사용되고 있다.

본 논문에서는 DRM 유통 시스템에서 인증서를 기반으로 하는 SSL 보안 통신 메커니즘을 제안하고, 이를 기반으로 한 암호 및 인증 서버/클라이언트의 설계 및 구현에 관하여 기술한다. 본 논문에서 제안된 SSL 보안 통신 메커니즘은 MS CryptoAPI를 사용하여 구현하였고, 인증서 기반의 보안이 필요한 다른 응용 프로그램(Messenger, ftp)에도 쉽게 적용 시킬 수 있는 특징을 가진다.

1. 서 론

최근 인터넷과 통신의 발전으로 인해 디지털 컨텐츠의 유통 및 이용이 증가하게 되었고, 이런 환경이 갖춰지고 시장이 형성됨에 따라, 기존 오프라인에서 서비스되고 있던 소프트웨어, 음반, 영화, 책등이 온라인에까지 영역을 넓혀 나가고 있으며, 전자상거래가 이루어지고 있다. 하지만 이런 컨텐츠를 소유한 사람들은 디지털 컨텐츠가 가지고 있는 ' 무작위 복제가 쉽다' 는 특성 때문에 사업화에 많은 어려움을 겪고 있다.

디지털 컨텐츠가 컨텐츠 이용을 위해 제약된 시간과 장소를 초월하여 자유롭게 이용할 수 있다는 장점이 있지만 원본이 허가 없이 수정되거나 재사용 될 수 있으며, 이렇게 만들어진 불법 컨텐츠가 엄청난 속도로 인터넷을 통해 배포됨으로써 저작 컨텐츠 소유자가 엄청난 피해를 입게 되고 유통 기업의 수익 창출에 어려움을 겪고 있는 것이 사실이다.

기존의 서버로부터 침입자를 감지하고 방어하는 개념, 바이러스 예방이나 파일에 대한 암호를 설정하는 기술 등 어떠한 것도 디지털 컨텐츠의 불법 복제를 해결해 주지 못했다. 이에 대한 해결 방안으로 디지털 컨텐츠 자체를 보호하여 저작권을 보호하고 저작권리자들의 수익 분배를 위해 관리 시스템을 제공하는 DRM 이 탄생하게 되었다[1]. 그러나 디지털 컨텐츠의 유통에 있어서 인증 및 통신의 무결성 등을 위한 보안은 아직도 매우 미흡한 상태이다.

DRM 의 탄생과 함께 가장 문제가 되는 부분이 어떤 보안 통신 메커니즘을 사용할 것인가의 중요성이 증대 되고 있다. 현재 PKI(Public Key Infrastructure)를 기반으로 하고 있는 SSL(Secure Socket Layer) 은 보안 통신을 위한 메커니즘으로 가장 많이 사용하고 있으며, 안정성이 매우 높다고 평가 되어 있다[2, 5]. 특히, SSL 은 어플리케이션에 독립적인 네트워크 레벨의 보안을 제공하며, 공개키 기반암호 통신 메커니즘 특성 때문에 현재 웹 환경은 물론이고 일반 기업에서도 자신의 어플리케이션 환경에 맞춰서 최적화된 SSL 을 활용하고 있다[3].

본 논문에서는 DRM 유통 시스템에서 인증서를 기반으로 하는 SSL 보안 통신 메커니즘을 제안하고, 이를 기반으로 한 암호 및 인증 서버/클라이언트의 설계 및 구현에 관하여 기술한다.

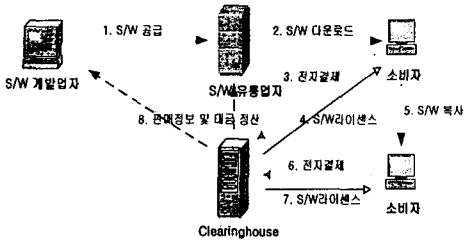
2. 관련 연구

2.1 DRM(Digital Rights Management)

DRM(Digital Rights Management)은 다양한 채널을 통해 유통되는 게임, 소프트웨어, 이미지, 전자서적, 음악파일, 영상정보 등의 각종 디지털 컨텐츠를 여러 형태의 불법 복제로부터 안전하게 보호하고, 이렇게 보호된 컨텐츠를 사용하게 함으로써 컨텐츠 서비스의 유료화를 가능하게 하는 기술이다[1].

DRM 은 단순히 불법복제만을 막는 기술이 아니라 안전 한 저작권과 승인내역, 권리와 승인의 집행, 인증된 환경과 서비스 인프라 등을 가능하게 하는 하드웨어와 소프트웨어를 모두 포함한 디지털 저작권 관리에 관련된 기술을 말한다[1]. [그림 1]은 DRM 을 이용한 일반적인 유통시스템의 구성도를 나타낸다.

소프트웨어 개발업자는 판매하고자 하는 소프트웨어를 유통업자에게 판매를 위탁한다. 유통업자들은 배포하고자 하는 소프트웨어의 상품 정보를 판매 사이트에 등록하고 해당 소프트웨어를 암호화한다.



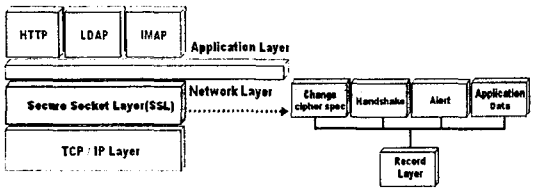
[그림 1] DRM 유통시스템의 구성도

소비자들은 소프트웨어 판매 사이트에서 원하는 상품을 선택하여 다운로드 받거나, 타 사용자의 소프트웨어를 카피하는 등의 배포가 가능하다. 하지만 소프트웨어를 사용하고자 하는 소비자는 결제과정과 적절한 사용권한을 받아야 하며, Clearinghouse 는 이 일을 관리하는 서버이다. 판매 결제 정보는 다시 소프트웨어 개발자로 전달되고, Clearinghouse 는 지속적으로 사용자를 관리한다[4].

2.2 SSL(Secure Socket Layer) 프로토콜

SSL 은 넷스케이프에서 개발한 보안 프로토콜로 TCP/IP 위에서 송수신자사이의 통신에 있어서 비밀성과 데이터 무결성 제공을 목적으로 개발 되었다.

본 논문에서는 DRM 은 [그림 1]과 같이 웹 상으로 자료를 전송하기 때문에 SSL 을 사용한다[5].



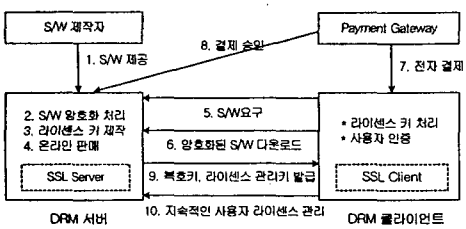
[그림 2] SSL 프로토콜의 구성

SSL 은 크게 핸드쉐이크 프로토콜과 레코드 프로토콜로 되어있고, 핸드쉐이크 프로토콜은 다시 Change cipher spec protocol, handshake Protocol, Alert Protocol, application Protocol 나누어진다. [그림 2]와 같은 일련의 과정 동안 보안 서비스를 위한 세션키, 암호 알고리즘, 인증서 등과 같은 변수를 서로 공유해야 하며, 이 정보를 이용해 레코드 프로토콜에서 실질적인 보안 서비스를 제공한다[5].

3. SSL 을 이용한 암호 및 인증모듈 구성

3.1 DRM 서버와 클라이언트 설계

[그림 3]은 본 논문에서 제안한 SSL 을 이용한 DRM 서버 및 클라이언트의 구성도를 나타낸다.



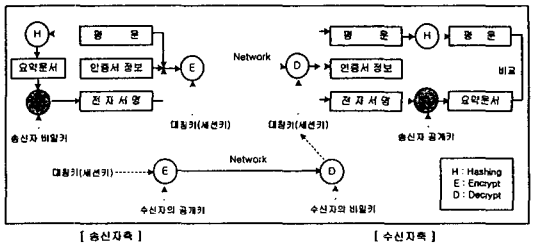
[그림 3] DRM 유통시스템의 구성도

DRM 서버는 SSL 서버를 포함하고 있으며, 주로 S/W 암호화 처리와, 라이센스키 제작, 온라인 판매를 담당하며 클라이언트로 부터 S/W 의 요구가 있을 경우 전자 결제승인 여부를 체크한 후 S/W 다운을 허용하고 지속적으로 라이센스를 관리하는 역할을 한다.

DRM 클라이언트는 SSL 클라이언트를 포함하고 있으며, SSL 클라이언트는 프로그램을 실행할 경우 정당한 사용자인지 판별하기 위한 정보를 서버에 전달하여 지속적인 라이센스 관리가 가능하도록 설계하였다.

3.2 암호 및 인증 모듈의 구성

[그림 4]는 SSL 을 기본으로 한 암호 및 인증 모듈의 구성도를 나타낸다.



[그림 4] 암호 및 인증모듈 구성도

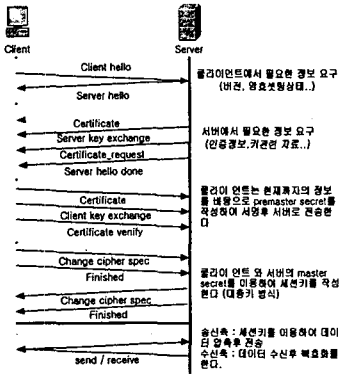
송신자측의 평문은 해쉬 알고리즘을 이용하여 문서요약 부분을 얻어 내어 이것을 무결성 검증 및 전자 서명에 사용한다. 인증서 정보는 중간에 악의적인 공격으로 인하여 서명문 자체를 변경하는 부분을 방지 하기 위한 조치이다. 이 과정을 모두 마친 후 평문, 인증서정보, 전자서명을 대칭키로 암호화하고 이 부분에 사용하였던 대칭키는 비대칭키 방식을 통하여 수신자 측에 전달 한다.

수신자측에서는 비대칭키 방식으로 암호화 하여 전달된 대칭키를 자신의 비밀키를 이용하여 복호하고, 복호된 대칭키를 이용해 암호문을 복호화 하고, 복호화된 인증서 정보를 바탕으로 평문은 해쉬 알고리즘을 이용 하여 요약문서를 얻어내고, 전자 서명은 송신자의 공개키를 사용하여 복호화 하여 요약 문서를 얻어내고 두 요약 문서를 비교하여 동일할 경우 통신중에 메시지 전달이 정상적이였다는 것을 나타낸다.

위에서 사용되는 대칭키를 제외한 송신자/수신자 공개키 비밀키는 모두 인증서 형식으로 저장되어 있는 키를 이용한다.

3.3 SSL 서버와 클라이언트 설계

[그림 5]는 본 논문에서 제안한 SSL 서버와 클라이언트의 통신 메커니즘을 나타낸다.



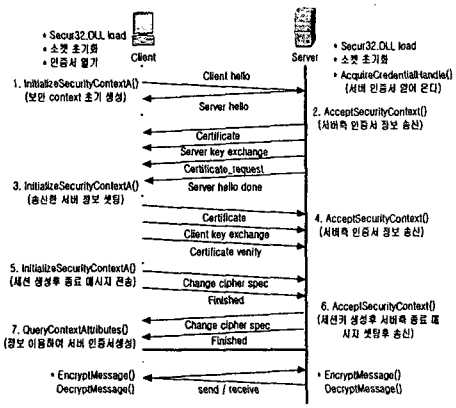
[그림 5] SSL 서버와 클라이언트의 통신 메커니즘

본 논문에서는 공개키를 이용한 암호화 방식에서 문제시되고 있는 속도 저하 문제를 해결하기 위하여 [그림 5]에 나타난 바와 같이 클라이언트와 서버 정보는 서버 인증서를 이용한 공개키 방식으로 전송하고, 이 정보를 이용하여 대칭키 (세션키)를 생성한다. 이 대칭키는 송신자/수신자 측에서 데이터를 암복호화하는데 사용된다.

4. SSL 서버와 클라이언트의 구현 및 실행 결과

4.1 구현 결과

[그림 6]은 [그림 5]에서 제안된 보안 통신 메커니즘을 기본으로 하여 SSL 서버와 클라이언트 구현 절차를 나타낸다.



[그림 6] SSL 서버 클라이언트 구현도

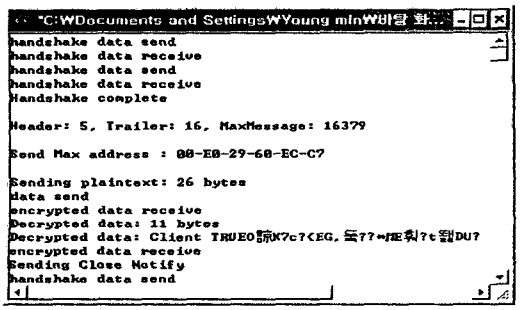
시스템은 MS CryptoAPI 를 기본으로 하여 구현되었으며, handshaking 전에 DLL 로드와 소켓 초기화 등이 필요하지만, 본 논문에서는 주로 SSL 과 관련된 부분에 대해서 설명한다.

우선 클라이언트에서 InitializeSecurityContextA()를 호출하여 보안 context 를 생성한 후 서버 측으로 전송하면, 서버 측에서는 클라이언트로부터 요구된 정보를 Accept SecurityContext()를 호출하여 setting 하고 다시 전송하는 과정을 반복하면서 세션을 생성한다. 생성이 끝나면 종료 메시지를 클라이언트와 서버 측에 각각 전달함으로써 모든 handshaking 과정이 끝나게 된다.

Handshaking 과정이 끝나면 세션 키가 생성되고 이 대칭키(세션키)를 이용하여 암호 및 복호화를 하면서 통신을 하게 된다.

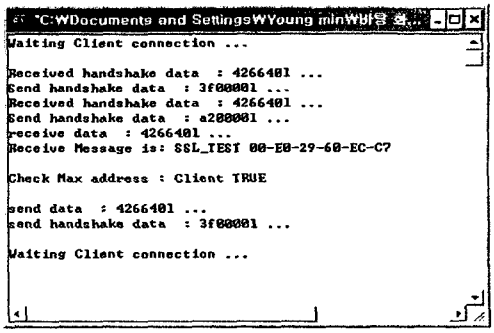
4.2 실행 결과

MS CryptoAPI 를 이용하여 구현한 클라이언트와 서버의 실행 결과는 각각 [그림 7]과 [그림 8]과 같다.



[그림 7] SSL 클라이언트

우선 클라이언트 부분에서 handshaking 이 성공하면 하드웨어 정보를 암호화하여 전송한다.



[그림 8] SSL 서버

이후 SSL 서버 측[그림 8]에서는 클라이언트에서 전달된 메시지를 복호화 하여 내용을 비교하고 결과에 따라 " Client True" , "Client False" 메시지를 전송하면 클라이언트는 전송받은 정보를 이용하여 실행 프로그램의 종료 여부를 결정한다. 위와 같은 방식으로 DRM 서버와 클라이언트 부분에서 SSL 이 사용된다.

5. 결 론

본 논문에서는 DRM 유통 시스템에서 인증서를 기반으로 하는 SSL 보안 통신 메커니즘을 제안하였고, 이를 기반으로 한 암호 및 인증 서버/클라이언트의 설계 및 구현에 관하여 기술하였다. 본 논문에서 제안된 SSL 보안 통신 메커니즘은 MS CryptoAPI 를 사용하여 구현하였고, 인증서 기반의 보안이 필요한 다른 응용 프로그램(Messenger, ftp)에도 쉽게 응용할 수 있다. 그러나 본 논문에서 제안된 SSL 통신 메커 니즘은 SSL 의 속도문제를 고려하지 않았기 때문에 실제로 다수의 사용자가 사용하기에는 문제점이 있다. 이 부분이 추후 연구되어야 하며, 보안과 속도를 모두 만족하는 것이 SSL 의 소프트웨어적 구현의 관건이라 할 수 있다.

<참고 문헌>

[1] DRM Working Group, http://www.digicaps.co.kr.

[2]AAP, Digital Rights Management for Ebooks: Publisher equipments version 1.0, 2000.

[3] Chor, B., A. Fiat, and Naor, "Tracing Traitors", in Advances in Cryptology, Proceeding of CRYPTO '94, vol. 839 of Lecture Notes in Computer Science, Spinger_Verlag, pp 257-270, 1994.

[4] DRM Working Group, http://www.fasoo.com 제공 프로그램 심의 조정위원회 월간지, 2001.

[5] Sherif, M.H., Serhrouchni, A., Gaid, A.Y., Farazmandnia, F., " SET and SSL: electronic payments on the Internet," ISCC '98. Proceedings. Third IEEE Symposium, pp. 353 □ 358, , 1998 .

[6] 강선영저 Visual C++암호화 프로그래밍, 프리렉, 2002.