2000년 한국정보처리학회 춘계 학술발표논문집 제7권 제1호

UML을 이용한 불법 복제 방지를 위한 ESD 서버 설계

윤우성*, 김태윤*
*고려대학교 컴퓨터학과
e-mail:wsyoon@netlab.korea.ac.kr

Design of ESD server to protect illegal copy using UML

Woo-Seong Yoon*, Tai-Yun Kim*
*Dept of Computer Science and Engineering, Korea University

요약

최근 초고속 통신망을 이용한 인터넷의 대중화와 더불어 인터넷을 기반으로 하는 전자 상거래가 활발해지고 있다. 특히 인터넷을 통한 소프트웨어 형태의 디지털 상품을 판매하는 전자 소프트웨어 분배(Electronic Software Distribution)는 전자 상거래 매출에 있어서 빠른 성장률과 높은 거래량을 기록할 것으로 평가되고 있다[1].

본 논문은 이러한 객체지향 기술중 통합된 모델링 방법인 UML을 이용하여 디지털 상품 불법 복제 방지를 위한 ESD 서버를 설계하였다. 불법 복제 방지를 위한 ESD 서버는 사용자에게 분배하는 사용권을 사용자 공개키를 이용하여 암호 알고리즘을 적용하여 분배한다. 따라서 소프트웨어형태의 디지털 상품의 불법 복제를 차단하는 효과가 있다.

1. 서론

사용상의 편의성과 초고속 통신망의 확산으로 인하여 인터넷 사용자가 급격하게 증가하였다. 또한 인터넷을 이용한 전자 상거래(Electronic Commerce)가 국내외에서 최대 관심사로 부각되고 있으며, 인터넷 전자 상거래가 본격화되면서 각종 컴퓨터 응용 패키지, 멀티미디어 동영상, 다양한 장르의 디지털 음악 파일, 문서 파일, 소프트웨어 등 유용한 디지털 정보 서비스를 상품화한 온라인 판매가 가능하게 되었다. 특히, 인터넷을 통한 디지털 상품(Digital Products) 유통은 저렴한 유통 방법에 의한 상품 가격의 인하와 물류 및 유통망 비용 절감을 통한 가격 경쟁력 획득이라는 여러 가지 부가적인 이득을 가지고 있다. 그러나 인터넷이라는 불완전한 개방형 전산망(Public Network)에서 전자 소프트웨어 분배(Electronic Software Distribution)를 안전하게 실현하기 위해서는 개인 정보 노출 또는 변조의 위험성을 최소화하며 정품에 대한 불법 복제 사용을 방지하는 것이 필수적이다[1]

본 논문은 이러한 객체지향 기술중 통합된 모델링 방법인 UML을 이용하여 디지털 상품 불법 복제 방지를 위한 ESD 서버를 설계하였다. 불법 복제 방지를 위한 ESD 서버는 소프트웨어의 판매형태인 디지털 상품을 공개키 암호 라이브러리를 사용하여 디지털 상품을 패키지한다. 사용권은 구매자의 공개키와 유통서버의 비밀키로 암호화하여 전자 메일로 전달한다. 구매자에게 분배하는 사용권을 가진 사용자만이 이 디지털 상품을 사용할 수 있다. 따라서 소프트웨어형태의 디지털 상품의 불법 복제를 차단하는 효과가 있다.

본 논문의 구성은 다음과 같다. 2장에서 객체지향 방법론인 UML과 전자 소프트웨어 분배인 ESD를 소개한다. 3장에서 유통 서버와 ESD 서버의 요구분석을 알아본다. 4장에서 UML을 이용한 불법 복제 방지를 위한 ESD 서버를 설계한다. 5장에서 결론 및 향후과제를 기술한다.

2. 관련연구

2.1 UML

현재의 정보시스템은 복잡화, 대형화, 전략 정보 시스템화로 발전해 오면서 과거의 개발방식으로는 대응하기가 매우 어려워졌다. 이에 따라 고수준의 소프트웨어를 개발하고 재사용과 유지보수를 지원할 수 있는 새로운 소프트웨어 개발 방법론이 요구되었으며 이로 인해 등장한 것이 객체지향 방법론이다[2][3]. 초기의 객체지향 개발 방법론

들은 시스템 모델링 및 문서화 부분에서 개발자에게 효과적인 방법을 제시하였으나, 각 방법론들의 다이어그램 및 표기법이 표준화되지 못하여 오히려 혼란을 야기시켰다. 이로 인해 객체지향 방법론의 표준화 작업이 필요시되어졌으며, 1995년 Grady Booch, James Rumbaugh, Ivar Jacobson등 객체지향 기술의 권위자들에 의해 통합 개발 방법론인 UML(Unified Modeling Language)이 제안되어졌다[4].

UML은 요구 분석, 시스템 설계, 시스템 구현 등 일련의 과정에서 사용되는 모델링 언어로서 이 세 단계 과정에서 발생하는 개발자간의 의사 소통의 불일치를 해소할 수 있다. 또한 모델링에 대한 표현력이 강하고 비교적 모순이 적은 논리적인 표기법(notation)을 가진 언어라는 장점도 갖는다. 따라서 개발자간의 의사 소통이 쉬워지며 생략되거나 불일치되는 모델링 구조에 대한 지적도 용이하다. 물론, 개발하려는 시스템 규모가 크거나 작거나 상관없이 모두 적용가능 하다[5].

2.2 ESD

전자 소프트웨어 분배(Electronic Software Distribution)는 불완전한 개방형 네트워크인 인터넷상에서 지적 재산권자와 판매자 그리고 사용자간의 소프트웨어 상품의 온라인 판매, 구매 방식을 의미한다[6,7].

ESD는 암호화 이론과 네트워크 보안 관리 기술을 통한 신뢰성 있는 온라인 판매 모델을 제시한다. ESD가 제공하는 신뢰성 있는 온라인 판매 모델은 다음과 같다. 사용자는 원하는 소프트웨어를 즉시 다운로드 할 수 있다. 하지만 허가된 사용자가 아니고서는 소프트웨어를 설치할 수 없다. 정품 소프트웨어의 사용을 위해서 사용자는 등록과 지불 과정을 마친 후 소프트웨어 사용권을 전달받아야 한다. 일련의 과정을 마치고 나면 다운로드한 소프트웨어의 설치시 락(lock)을 풀 수 있는 사용권을 전자 메일을 통해서 사용자에게 제공한다. 물론 사용권은 암호화되어 있어서 전자 메일을 가로채더라도 사용자가 아니면 암호를 풀 수 없다. ESD를 사용하는 하는 대표적인 상용 기술로는 시멘텍(SYMANTEC)사에서 이용되는 기술을 들 수 있다.

ESD는 지적 재산권자, 판매자, 사용자 모두에게 상품 가격의 인하와 물류비용 및 유통망 비용 절감을 통한 가격 경쟁력 확보 등의 여러 가지 부가적인 이득을 제공한다.

3. 요구분석

3.1 구매자 요구 분석

- 디지털 상품 쇼핑 및 설치가 용이해야함
- 구매 및 사용자 정보 등록시 개인 정보가 보호되어야 함
- 구입한 상품은 추후 업그레이드 받을 수 있어야 함
- 정품을 구매한 사용자라는 인증이 가능해야 함

3.2 지적 재산권자 요구 분석

- 디지털 상품의 판매 정보를 얻을 수 있어야 함
- 구매자와의 피드백이 가능해야 함
- 불법 사용자에 대한 판매자와 구매간의 책임 규명이 가능해야 함

3.3 유통 서버 요구 분석

- 개인 정보와 신용 정보의 누출이 없어야 함
- 추후 A/S를 위한 반품 정보 처리 및 관리 기능이 있어야 함
- 지적 재산권자에게는 새로운 상품을 등록하는 작업이 편리해야 함
- 현재까지의 판매 상황에 대한 통계 기능이 있어야 함

3.4 ESD 서버 요구 분석

- ESD 서버는 기존의 유통 서버의 기능을 모두 가지고 있어야 함
- 사용권을 가진 사용자만 디지털 상품을 수행 할 수 있어야 함
- 사용권을 전달받은 사용자가 디지털 상품을 산 구매자가 맞는가를 인증해야 함
- 구매자가 디지털 상품을 불법 배포하는 것을 방지해야 함

4. UML을 이용한 ESD 서버 설계

4.1 ESD 서버의 구성

그림 1 은 ESD 서버의 전체 구성을 나타낸다.

ESD 서버에서 요구된 사항은 불법 복제 방지를 위한 상품 패키지와 사용권을 제작 및 분배하는 상품 제작 모듈이다.

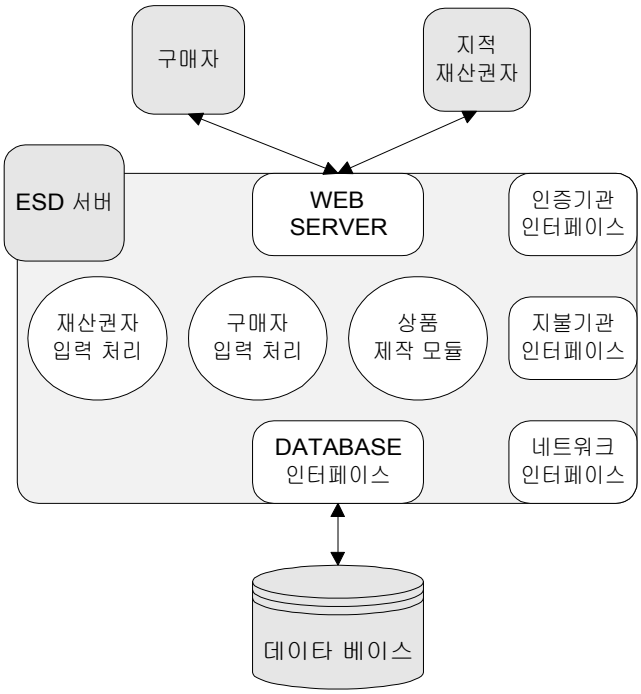

그림 1 ESD 서버의 구성

상품 패키지에는 실행 파일과 사용권 확인 쓰레드가 담겨져 있다. 사용자가 이 패키지를 실행하면 실행 파일이 실행되는 동시에 사용권 확인 쓰레드가 동작한다. 사용자가 전달받은 사용권이 인증되면 실행 파일이 동작하고, 인증되지 못하면 사용권 확인 쓰레드가 실행 파일을 강제로 종료시킨다. 즉 사용권을 가진 사용자만이 디지털 상품을 수행 할 수 있다.

ESD 서버에서 상품을 제작하고 분배하는데 적용하는 암호 알고리즘은 공개키 암호 방식을 이용한다. 공개키 암호 방식에는 공개키(P:Publicy Key)와 비밀키(S:Private Key)가 있다.

사용권($S_{유통서버}(P_{사용자}$(상품코드)))은 상품마다 유일한 값인 상품코드를 담고 있다. 이 상품코드는 상품의 값을 지불한 구매자의 공개키로 암호화하고 유통서버의 비밀키로 암호화한다. 상품코드를 사용자 공개키로 암호화하므로 사용권을 전달받은 사용자만 암호를 해독 할 수 있다. 유통서버의 비밀키로 암호화하므로 구매자가 상품코드를 다른 사용자에게 전달하는 것을 막는다.

4.2 Use case diagram

Use case는 사용자 입장에서 본 시스템의 행동을 일컫는다. Use case는 ESD 서버 시스템에서 사용자가 원하는 사항을 얻어내는데 매우 유용하다.

구매자의 행위는 상품 구매 신청을 할 수 있고, ESD 서버로부터 상품을 전송 받을 수 있다. 사용권 전송의 경우 ESD 서버에서 사용자의 지불 처리가 종료된 후 발생하는 트랜젝션이다.

지적 재산권자는 상품 등록 요청 행위를 한다.

ESD 서버는 구매자와 지적 재산권자가 발생한 행위에 대하여 먼저 사용자 확인 처리를 해야 한다. 지적 재산권자가 발생한 행위에 대하여 상품 저장 처리를 해야 하고, 구매자가 발생한 행위에 대하여는 상품을 제작하고 이를 구매자에게 전송해야 한다. 그림 2는 사용자의 행위에 입각한 ESD 서버의 Use case diagram이다.

4.3 Class diagram

공통적인 특성을 가진 것에 대하여 실세계에서는 범주로 묶을 수 있는데, 클래스는 바로 이 범주의 개념이다. Class diagram은 시스템 내에 존재하는 각 클래스들의 인터페이스와 클래스 사이에 맺어지는 다양한 정적인 관계를 표현하는 다이어그램이다.

UML에서 클래스를 나타내는 아이콘은 세 부분으로 쪼개져 있다. 가장 윗 영역은 클래스의 이름을 넣고, 둘째 영역은 속성을 넣는 공간 그리고 가장 마지막 영역은 오퍼레이션을 넣는 공간이다.

User_Certificate 클래스는 사용자의 정보를 확인하고 ESD 서버에서 상품 패키지를 제작하는데 필요한 정보를 제공하는 클래스이다. User_Certificate 클래스는 Send_product 클래스와 Source_manage 클래스에 메시지를 전달한다.

Make_product 클래스는 상품 패키지와 사용권을 제작하는 클래스이다. Send_product 클래스는 Make_product 클래스를 상속받아서 상품 패키지와 사용권을 구매자에게 전달한다. 그림 3은 ESD 서버의 Class diagram이다.

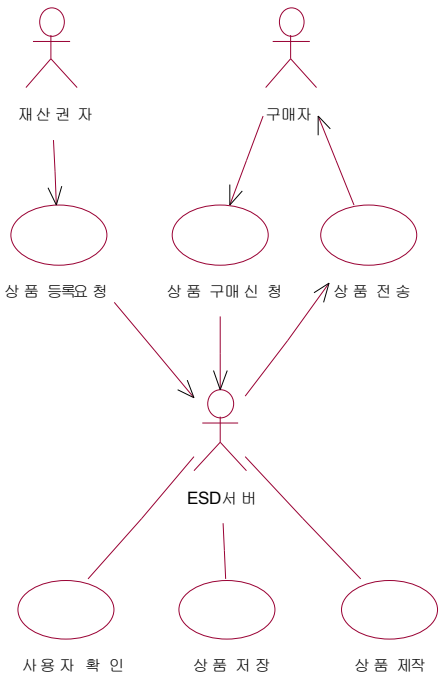

그림 2 User case diagram

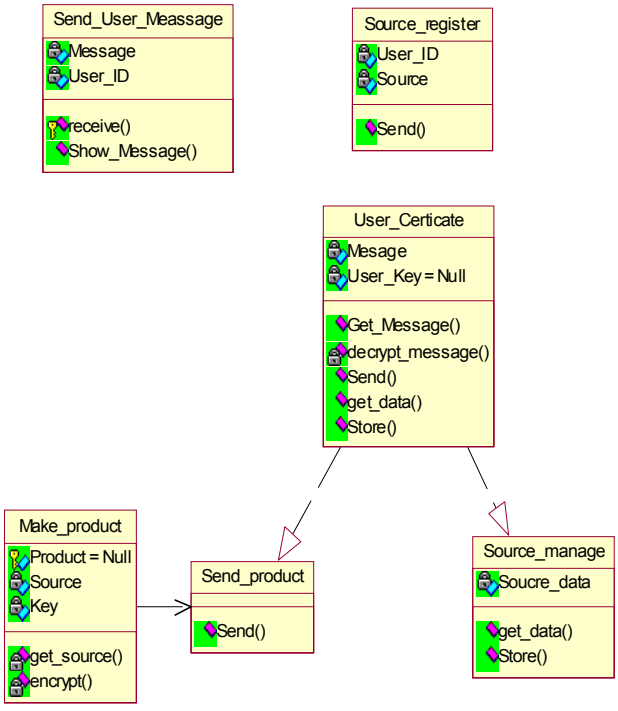

그림 3 Class diagram

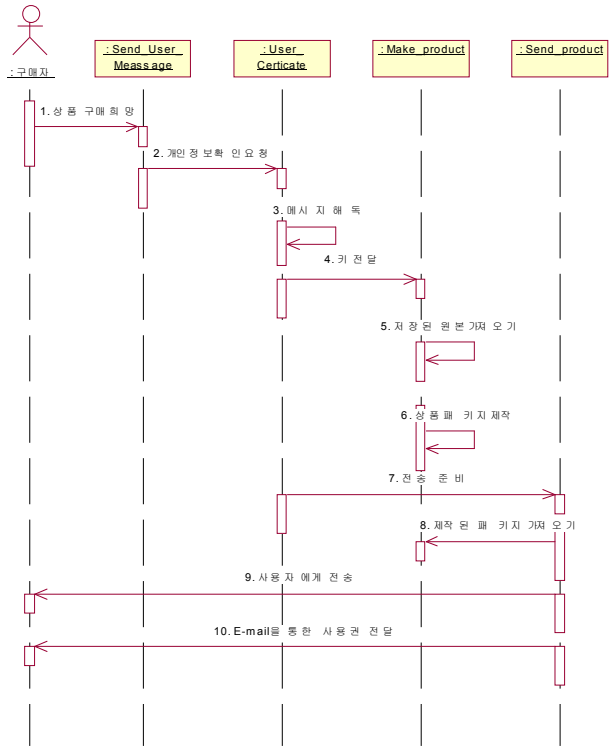

그림 4 Sequence diagram

4.4 Sequence diagram

앞서 살펴본 Use case diagram과 Class diagram은 시스템의 정적인 정보를 나타낸다. 그러나 ESD 서버 시스템은 여러 개의 객체들이 서로 메시지를 주고받으며 작업을 진행하는 것이 보통이다. Sequence diagram은 객체들끼리 주고받는 메시지의 순서를 시간의 흐름에 따라 보여주는 것이다. ESD 서버에서 Sequence diagram은 구매자가 상품 구매 신청을 한 후 상품이 전달되기까지 객체들의 순서적인 작업을 나타낸다. ESD 서버의 순서적인 작업은 다음과 같다. 그림 4은 ESD 서버의 Sequence diagram이다.

① 상품 구매 희망 및 개인 정보 전송
② 개인 정보 확인 요청
③ 전달된 메시지 확인 및 상품 제작 준비
④ 사용자 공개키(P) 전달
⑤ DB에 저장된 상품 원본 읽어오기
⑥ 상품 패키지 와 사용권 제작 및 저장
⑦ 전송 준비 알림 및 정보 전달
⑧ 전송할 제작된 패키지 가져오기
⑨ 상품 패키지 사용자에게 전송
⑩ E-mail을 통한 사용권 전달

5. 결론 및 향후 과제

ESD를 기반으로 하는 디지털 상품의 효율적이며 안전한 분배에 관한 연구가 활발해 지고 있다. 본 논문에서는 UML을 이용하여 암호화 기법을 적용하여 디지털 상품의 불법 유통을 차단할 수 있는 ESD 서버를 설계하였다.

불법 복제 방지를 위한 ESD 서버는 사용권을 가지고 있는 사용자만 상품을 사용할 수 있다. 현재 사용권 소유자가 구매자인 것을 인증 한다. 사용자가 디지털 상품을 불법 배포하는 행위를 방지할 것을 보장한다.

향후 연구과제로는 인증 절차를 줄여 암호화 라이브러리를 사용하는데 소요되는 시간 오버헤드를 줄이는데 있다.

참고문헌

[1] "ESD", URL : http://www.siia.net/pubs/bookstore/items/wpe98.htm
[2] James Rumbaugh, "Object-Oriented Modeling Technology (OMT)", Tutorial, OOPSLA'94
[3] Ivar Jacobson, "Object-Oriented Software Engineering", Addison-Wesley, 1994
[4] Eriksson, Penker "UML Toolkit", Wiley, 1998
[5] “UML overview", URL : http://members.tripod.co.kr/ymyang/uml/overview.htm
[6] "Electronic Commerce for Software", URL : http://www.globetrotter.com/ecs1.htm
[7] "A Guide to Electronic Commerce and Digital Distribution" URL : http://208.240.131.116/get-started/index.html