

동적 사용권 관리를 이용한 소프트웨어 상품의 온라인 유통

강 우 준[†] · 김 응 모^{††}

요 약

전자상거래가 활성화되면서 인터넷을 이용한 상품의 구매가 점점 증가하고 있다. 현재 전자상거래에 이용되는 대부분의 상품은 하드웨어가 주를 이루고 있다. 전자파일 형태의 상품 즉, 디지털 상품의 온라인 판매는 물류비용이 없고, 상품의 검색이 용이하며, 한시적으로 사용해 본 후 구입할 수 있는 등의 많은 장점을 가지고 있지만 불법 복제 문제 때문에 현재 전자상거래에서는 기피 상품으로 취급받고 있다. 디지털 소프트웨어 상품의 불법 복제 문제는 사용권 관리 기술의 부재가 가장 큰 이유중의 하나이다. 현재 이루어지고 있는 전자상거래는 사용권 부여 대상의 식별 방법이 없고, 대상의 이동 방지가 불가능하고, 해킹 방지가 미비하며, 기타 전자상거래 구조가 미완성되어 사용권 관리상에 많은 문제점을 드러내고 있다.

본 논문에서는 전자상거래 상에서 소프트웨어 상품의 유통을 활성화 할 수 있는 새로운 사용권 관리 기술인 동적 사용권 관리(DLC : Dynamic License Control) 기술을 이용하여 디지털 상품의 유통을 활성화 할 뿐 아니라 불법 복제를 막을 수 있는 디지털 소프트웨어 상품의 상품 작성 시스템의 설계 및 구현을 제안한다.

On-line Circulation of Software Product based on Dynamic License Control

Woo-Jun Kang[†] · Ung-Mo Kim^{††}

ABSTRACT

Internet purchase is increasing according to the activation of Electronic Commerce. Currently, the hardware is main purchase items in the Electronic Commerce. The on-line purchase of digital product, that is electronic file type of product, has many merits such as, does not cost in logistics, is ease of searching the product, and is possible of 'Try and Buy' system. But, actually digital products have not been major product because of its piracy problem. The piracy problem of digital products comes from the lack of safety in DP license control technology. Current EC has no method to identify the object that has the right to use the digital product. The protecting of object change is impossible and the protection of hacking is not enough and EC has many problems in efficient license control because of the incompleteness of EC structure.

In this paper, we propose the design and implementation of on-line DP circulation system, which can activate on-line circulation of DP in EC and protect its piracy, by using the new license control technology, that is Dynamic License Control technology.

[†] 정 회 원 : 안산공과대학 전산정보과 교수

^{††} 종신회원 : 성균관대학교 전기전자 및 컴퓨터 공학부 교수
논문접수 : 2000년 3월 31일, 심사완료 : 2000년 4월 19일

1. 서 론

인터넷 웹 기술의 발달로 인한 인터넷의 대중화가 시작되어 고속화가 실현되면서 인터넷 전자상거래가 점차 확산되어 가고 있다. 이에 따라 기존의 하드웨어 중심의 구매는 물론 각종 컴퓨터 응용 소프트웨어, 멀티미디어 상품들이 전자파일 형태로 판매가 가능하게 되었다[14]. 전자파일의 온라인 판매는 물류비용이 들지 않고 사용자들이 사용해 본 후 구매를 결정할 수 있으므로 판매가 신장되는 등 수익성이 높으나 불법 복제의 문제로 인해 현재는 전자상거래에 있어 기피 상품으로 여겨지고 있다. 이 문제는 완벽한 사용권 관리와 효율적인 온라인 유통이 없이는 해결할 수 없는 어려움 가운데 놓여있다. 현재 전자상거래에 있어 사용권 관리상의 문제는 사용권 부여 대상의 식별 방법이 없고, 대상의 이동방지가 불가능하며, 오늘날 모두의 관심의 초점이 되고 있는 해킹 방지에 있어서도 미비하며, 현재까지 전자상거래 구조가 완성되지 못한 데에서 기인한다[15].

인터넷이 일반화되고 전자상거래 기반이 출범되며, 각종 사이버 범죄를 막을 수 있는 공개키 암호화 기술이 등장하고, 전자 파일의 원활한 유통에 필수적 요소인 네트워크의 속도가 고속화되고 있는 새로운 환경으로 접어들면서 전자파일 형태의 디지털 상품에 대한 구매욕구와 필요성이 급격히 커지고 있다. 이러한 디지털 상품으로는 각종 컴퓨터 응용 소프트웨어, 멀티미디어 동영상, 다양한 장르의 디지털 음악 등을 들 수 있다[13, 17]. 디지털 소프트웨어 상품의 유통에 있어 개선되어야 할 가장 중요한 요소는 불법 복제를 근본적으로 해결해 줄 수 있는 사용권 관리에 있다.

본 논문의 구성은 2장 디지털 소프트웨어 상품의 유통을 위한 요구사항에 관하여, 3장에서는 세계의 사용권 관리 기술을 간략히 소개하고 4장에서는 동적 사용권 관리(DLC : Dynamic License Control) 기술의 구조 및 이를 이용한 디지털 소프트웨어 상품의 유통 시나리오, 5장에서는 상품 작성 시스템의 설계, 6장에서는 소프트웨어 유통 시스템의 구현, 7장에서는 결론 및 향후 연구 과제를 논한다.

2. 디지털 소프트웨어 상품의 유통을 위한 요구사항들

물류의 이동이 없이 유통이 가능한 디지털 상품은

크게 소프트웨어 상품과 연결 프로그램에 의해 수행되는 데이터인 디지털 데이터 상품으로 나눌 수 있다. 특히 디지털 데이터는 수행결과를 가지고 내용을 만들어 낼 수 있다는 점에서 소프트웨어 상품과는 전혀 다른 특징을 가지고 있고 높은 가격으로 유통이 불가능하다. 하지만 소프트웨어 상품은 수행 결과를 가지고 소프트웨어 상품을 만드는 Reverse Engineering이 불가능하므로 상품의 보호가 완벽히 이루어질 수 있고 가격도 여러 가지의 범주를 가질 수 있어 디지털 상품 중에 가장 좋은 유통 대상이라고 할 수 있다. 따라서 다른 어떤 분야보다도 가장 많이 사용권 관리 기술에 대한 개발 노력이 이루어져 왔다고 할 수 있다.

이러한 소프트웨어 상품을 대상으로 오늘날 많은 기업이 전자상거래에 참여하여 많은 실적을 거둘 수 있었던 데에는 사용권 관리의 기반 기술들 중의 하나라고 할 수 있는 거래 당사자간의 정보 내용에 대한 암호화 기술이 가장 중요한 역할을 하였다고 볼 수 있다.

암호화 기술 중 공개키 암호 기술의 개념은 1976년 W. Diffie와 M.E. Hellman이 처음 소개하였다[3]. 2-key 또는 비대칭 암호 방식(asymmetric cryptosystem)으로도 불리는 공개키 암호 시스템은 각 사용자가 하나의 비밀키를 공통으로 사용하는 비밀키 암호 시스템과는 다른 점이 많다. 1976년 Diffie와 Hellman이 공개키 암호 방식의 개념을 발표한 후, 1978년 MIT의 Rivest, Shamir와 Adelman이 처음 RSA라고 하는 유망한 공개키 암호 방식을 제안하였다[4]. 암호화 할 때 사용하는 공개키는 공개된 파일 상에 전화 번호처럼 공개하고, 복호화 할 때 사용하는 비밀키는 안전하게 보호되어야 하는 키다 [5-9].

공개키 암호 시스템과 함께 중요한 요구사항 중의 하나는 해킹 방지 기술이라 할 수 있다. 동적 사용권 관리 시스템에 있어 각 상품과 사용권 관리 프로그램과의 연결 부분에 있어 해킹의 위험성이 없어야 한다. 해커들의 불법적인 해킹을 막는 방법에 대한 연구도 지속적으로 이루어져야 한다.

또한 배포된 소프트웨어 상품에 대해 정당한 사용권 관리를 하기 위해서는 효율적이고 편리한 상품 작성 방법이 무엇보다 중요하다. 원시 상품에 대한 훼손이나 퍼포먼스 등에 영향을 미치지 않고 사용자의 입장에서 쉽게 사용할 수 있도록 하는 상품 작성이 이루어져야 하는데 본 논문에서는 이에 대한 방법들을 제시하고자 한다.

소프트웨어의 경우에는 상품의 수행 결과를 가지고 상품 자체를 재생하는 것이 불가능하며 상황에 따라 다른 동작을 하기 때문에 소스(source) 없이는 소프트웨어 상품의 해독, 변형 및 Reverse Engineering이 매우 힘들다.

이러한 특징들을 고려해 볼 때 소프트웨어 상품 유통의 이상적인 모델은 다음과 같은 여러 가지 조건들을 갖추어야 한다.

첫째, 무료 사용 기간이 제공되어 사용자들이 제품을 손쉽게 다운로드하여 제품을 사용할 수 있어야 한다.

둘째, 유료 소프트웨어의 전제 조건으로는 구매절차와 대금 지불절차 및 사용권 관리가 완벽하게 이루어져야 한다.

셋째, 유료 소프트웨어로서 반드시 추가 시켜야 하는 절차들에 대해 최대한 효율적인 관리가 유통 시스템의 효율화의 가장 중요한 요소이다.

넷째, 사용 후 구매가 가능해야 한다. 즉, "Try & Buy"가 가능해야 한다. 특히 이 조건은 영업적인 측면에서 매우 중요하다. 또한 상품 배포가 용이하여 누구라도 손쉽게 상품을 획득하여 사용해 볼 수 있어야 한다. 이로써 상품 판촉에도 중요한 효과를 거둘 수 있어야 한다. 결국 상품을 사용할 때 최소 절차로 상품 구매가 가능해야 하는데 이는 제품을 임시적으로 소유한 상태에서 구매가 가능해야 한다는 것이다.

소프트웨어 상품의 유통을 위한 중요한 요구사항들을 정리해 보면 다음과 같다.

첫째, 완벽한 사용권 관리가 가능해야 한다. 즉, 불법 복제가 완전히 방지되는 안정된 시스템을 갖추어야 하며 변조 및 해킹이 불가능해야 하고 불법적인 사용을 방지할 수 있어야 한다.

둘째, 다양한 사용권을 제공하여 사용자들이 자유롭게 구매 조건을 선택할 수 있어야 한다. 예를 들면, 영구 사용권과 일정 기간 사용권 및 일정 회수 사용권의 구분이 가능할 뿐 아니라 누적 사용시간에 따른 사후 지불, 사용자의 수 및 사용자의 신분에 관련한 구분도 가능해야 한다. 즉, 학생용 사용권, 업그레이드 사용권, 직원 사용권 등에 대한 구분이 가능해야 한다. 또한 불법적인 행위를 한 사용자에 대해서는 사용권을 취소할 수 있어야 한다.

셋째, 효율적인 유통이 이루어져야 한다. 즉, 구매절차가 간단해야 하며 사용권 관리 절차도 간단해야 한다. 특히 저작사들의 유통 참여 절차가 손쉽고 간단해

야 한다.

넷째, 상품의 배포가 용이해야 한다.

다섯째, 상품에 대한 판촉이 손쉬워야 한다.

여섯째, 그 밖에 기증 절차 및 자산 관리와 같은 다양한 기능들이 필요하다.

소프트웨어의 유통에 있어서 사용권 적용에 관하여 좀더 살펴보면 다음과 같다. 소프트웨어 유통 시스템은 이 논문에서 제안하는 동적 사용권 관리 방식의 사용권 부여 대상 결정 방식 및 대상 식별 방식을 그대로 이용한다.

사용권 관리에 있어 중요한 요소를 살펴보면 다음의 세 가지로 분류할 수 있다.

첫째, 사용료에 관한 구분이다. 무료, 유료, 기증, 사용자 수 기준, 업그레이드, 학생, 일반을 구분할 수 있어야 한다.

둘째, 사용권의 종류를 구분할 수 있어야 한다. 즉, 영구 또는 일정기간 사용권을 들 수 있다.

셋째, 사용권의 취소가 가능해야 한다. 사용자의 불법적인 행위에 대해서는 사용권 취소가 가능해야 한다. 또한 사용권이나 신분증 갱신 시에도 이를 거부함으로써 사용을 통제할 수 있어야 하며 상품을 구매할 때부터 거부할 수도 있다.

3. 세계의 사용권 관리 기술

사용권 관리 기술은 각 디지털 상품의 특징에 따라 달리 처리해야 할 부분들도 있지만 많은 부분에 있어서 같은 접근 방법을 가져야 하는 부분들이 많다[11, 12]. 이 논문은 동적 사용권 관리 기술의 소프트웨어 온라인 유통에의 효율적인 적용에 대한 논문이나 디지털 상품 전체에 대한 사용권 관리 기술을 참고하였다. 디지털 상품의 유통은 크게 2가지 부분으로 나누어 볼 수 있다. 첫째 사용권 관리 부분과 둘째 상품의 작성 및 상품의 수행이다. 디지털 상품의 특성에 따라 상품의 작성 및 수행에는 차이가 있을 수 있으나 사용권 관리 기술 자체는 디지털 상품 분야와 무관하게 통합적으로 연구되어야 할 것으로 생각된다. 하지만 아직 대개의 소프트웨어와 MP3의 유통 관련 연구 성과는 공유되고 있지는 못하고 있어 각각의 진행 상태는 개별적으로 검토가 되어야 할 것으로 생각된다. 소프트웨어 분야에 있어 가장 주요한 연구는 주로 ESD(Electronic Software Distribution, 전자적 소프트웨어 유통)라는 주제 아래 진행되

어 왔다[14]. 국외에서 가장 앞선 유통 기술로 간주할 수 있는 것들은 대개 소프트웨어 유통 패키지로서 판매되어 소프트웨어 저작사들이 이를 구매 자신들의 소프트웨어 판매를 위한 독자적인 유통 시스템 설치에 이용되고 있다. 음악 분야도 근래에 국제적인 조직인 SDMI(Secure Digital Music Initiative)를 중심으로 음악 저작권 관리 기술 표준화에 대한 노력을 기울이고 있으며 아직은 매체의 복제 방지를 하려고 한다는 점에서 소프트웨어 분야보다 다소 낮은 수준이라고 할 수 있을 것이다. 이런 SDMI의 존재 때문에 음악 부분은 전세계 기술 수준을 파악하는데 많은 도움을 주고 있다. SDMI는 현재 여러 가지 개선을 해야 할 사항을 가지고 있지만 그 중 음악 매체의 복제 방지(Copy Protection of Portable Media) 시도는 대표적으로 잘못된 접근 방법이라고 생각된다. 이는 소프트웨어의 유통에서 궁극적 요소로 중요시하는 shareware 방식을 불가능하게 만들어 버린다. 이는 사용자가 필요로 하는 사용성을 크게 저하시킨다. 사용권 기술이 추구하여야 할 요소는 많지만 중요한 부분은 1) 안전성, 2) 사용성, 3) 기능성, 4) 효율성 측면에서 살펴 볼 수 있을 것이다. 지금까지는 사용권 관리 기술에 대한 안전성이 가장 큰 문제였기 때문에 기타 부분에 대해서는 아직 깊이 있게 논의되지 못하였다. 소프트웨어 불법 복제를 방지하는데 가장 앞장서는 조직인 BSA와 SIIA(이전 이름 - SPA)도 아직은 기술적인 문제 해결보다는 법적인 조처에 치중하고 있다[3, 9].

〈표 1〉 사용권 기술의 문제점

| 분 야 | 기술명 | 문 제 점 |
|-------|------|--|
| 소프트웨어 | ESD | 물킷으로 판매-사용성 및 효율성 문제 |
| MP3 | SDMI | 매체의 복제 방지-상품 배포 장애, 사용성 문제 |
| MP3 | AOD | 대금 지불 후 암호화-서버의 자원 침해, 네트워크 자원이 많이 필요. 상품 배포 방법 제한 |

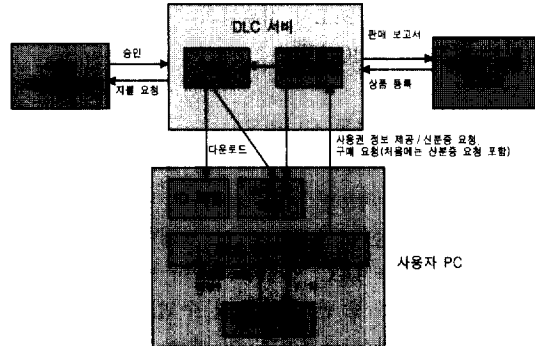
국내 음악 관련 기술은 AOD기술이라고 할 수 있으며 1999년에는 전자 부품 연구원이 주도하는 DMC(Digital Music Consortium)을 중심으로 국내 기술 표준을 만들기 위한 노력을 진행하였다[8]. 국내 AOD기술은 음악을 배포할 때 반드시 개별적인 암호화가 수행되어야 하고 온라인으로만 배포가 가능하다는 점에서 배포에 큰 제약이 있으며 유통 시스템의 운영에도 많은 자원이 요구되리라 생각된다[6]. 따라서 고객 사용성 부분과 유

통시스템의 효율성 측면에서 개선의 여지가 있다고 보여진다.

4. 동적 사용권 관리(DLC : Dynamic License Control) 구조 및 소프트웨어 유통 시나리오

4.1 DLC의 구조

소프트웨어의 유통 시스템은 (그림 1)과 같이 지불 게이 트웨이(PG : Payment Gateway), 유통 서버(DLC Server), 저작사(Digital Product Manufacturer), 사용자(User PC)의 4부분으로 이루어진다. 각 모듈을 살펴보면 다음과 같다[1].



(그림 1) 소프트웨어 유통 시스템을 위한 DLC의 구조

첫째, 지불 게이 트웨이는 DLC 서버로부터 지불 요청을 받고 그에 대한 응답을 DLC 서버에게 보내준다.

둘째, DLC 서버는 상품 유통 서버에 설치되어 사용권 관리와 DLC 클라이언트의 요청에 대한 답변을 담당한다. 또한 저작사에서 유통 서버에 상품을 등록하고 판매할 수 있는 인터페이스를 제공하며 저작사에게 판매 보고서를 제공하고 상품 판매와 지불에 대한 처리를 담당한다. CA(Certificate Authority)와 DP Mall로 이루어져 있다. CA는 디지털 서명을 하여 ID 파일과 사용권 파일을 암호화한다. DP Mall은 디지털 상품을 판매하고 사용자 PC에 사용권 파일을 다운로드 한다.

셋째, 저작사는 그의 상품을 저장한 후 DLC 서버에 상품을 등록하고, 유통 서버에서 제공하는 상품 작성 방식에 따라 상품을 제작한다. 이와 같이하여 상품 판매를 한 후 그에 따른 판매 보고서를 DLC 서버로부터 받게된다.

넷째, 사용자 PC에 있는 DLC 클라이언트는 사용자

로 하여금 상품을 구매할 수 있도록 인터페이스를 제공한다. 또한 상품을 사용할 수 있는 사용권에 대한 관리를 담당한다. ID 파일은 사용자의 비밀키를 가지고 있으며 사용권 파일은 모든 사용권 정보를 가지고 있다. DLC 클라이언트는 디지털 상품으로부터 그 사용자가 그 상품에 대한 사용권이 있는지의 여부를 묻는 질의를 받고 사용권 파일을 참조하여 가부간의 대답을 하게 된다. 사용권이 있는 경우는 해당 소프트웨어가 계속 수행되지만 그렇지 않을 경우는 그 즉시 수행이 중지된다.

DLC 서버와의 연결은 사용권 구입 시에만 필요하며, 일반적인 사용권 관리 시에는 DLC 서버와 연결되어 있을 필요가 없다. 이 시스템을 통한 사용권 관리는 Client/Server 구조로서 서로간의 통신은 TCP/IP를 통해서 이루어진다[10-12].

4.2 소프트웨어 유통 시나리오

(그림 1)에서 제시한 환경 하에서 소프트웨어의 유통 시나리오를 살펴보면 다음과 같다.

첫째는 상품 등록 단계이다. 이 단계에서는 저작사가 개발한 상품을 DLC 서버와 더불어 수행하는 과정으로 판매를 위한 첫 번 단계라 할 수 있다.

둘째는 상품 작성 단계이다. 이 때는 저작사가 상품 등록 시 받은 정보를 이용하여 상품을 작성하게 된다.

셋째는 상품 배포 단계이다. 저작사가 상품의 판매와 홍보를 위해 직접 또는 간접적으로 불특정 다수를 대상으로 배포한다. 특히 "Try & Buy" 방식의 경우에 있어서는 영업의 성과를 위해 매우 중요한 단계라 할 수 있다.

넷째는 상품 설치 단계이다. 사용자는 여러 경로를 통해 얻은 상품을 자신의 컴퓨터에 설치하여 사용해 보는 단계이다. 이때 시험적인 사용을 하게 되는데 사용자에게 불편을 주어서는 안되며 오히려 상품에 대한 매력을 느낄 수 있도록 주의를 기울여야 한다.

다섯째, 상품 구매 단계이다. 사용자가 DLC 서버와 수행하는 작업으로 설치된 상품에 대해 사용권이 없으면 연결 프로그램 또는 사용권 관리 프로그램이 구매 작업을 수행한다.

여섯째, 구매한 상품을 사용하는 단계로서 사용자 컴퓨터에서 수행되는 단계이다.

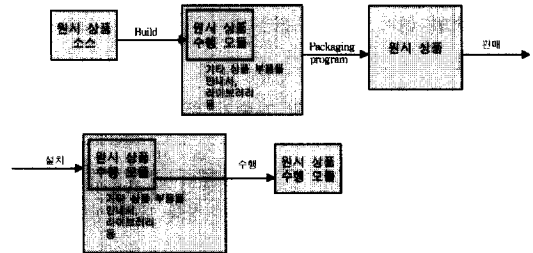
특히 설치 및 사용자 가입 단계에서는 사용자 컴퓨터에 사용자 프로그램을 설치하고 DLC 서버에 회원

가입을 하고 신분증을 받게 된다. 이 작업은 일생동안 단 한번만 수행하면 된다.

5. 소프트웨어 상품 작성 시스템의 설계

전자상거래 상에서 소프트웨어 상품의 온라인 유통을 실현하고자 할 때 효율적인 사용권 관리를 실현할 수 있도록 원시 상품 작성에 있어 4가지의 방식을 모델로서 제시하고자 한다.

(그림 2)에서 보여주는 기존의 방식에 있어서의 문제점은 다음과 같이 분석해 볼 수 있다. 첫째, 기존의 방식에서는 저작자가 원시 상품소스를 사용 시에 필요한 정보들과 함께 패키지화 하여 원시 상품을 만든 후 구매자에게 우편 등의 방법을 통하여 직접 보내게 되므로 물류비용과 일정한 기간이 소요된다. 둘째, 각종 영업망을 통하여 판매를 하게되므로 관련 유통 회사를 통한 영업망의 확보가 필요하며 그에 따른 비용도 발생하게 된다. 셋째, 이와 같은 방식으로 판매된 상품에 대해 불법적인 사용을 막을 수 있는 유일한 방법으로는 설치 시 해당 상품의 키 값을 확인하는 정도이다. 다시 말해서 해당 소프트웨어를 복제하고 키 값을 알고 있다면 무한정의 불법적인 복제가 이루어져도 아무런 대책이 없다.



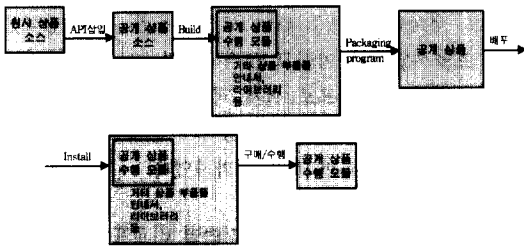
(그림 2) 기존의 상품 작성 및 수행 방식

이와 같은 문제점들 때문에 소프트웨어 상품의 저작사들은 막대한 비용을 들여 좋은 상품을 개발해 놓고도 그에 상응하는 이윤을 얻지 못하고 있는 것은 커다란 문제라 아니할 수 없다.

사용권 관리의 획기적인 방법이 없이는 이와 같은 문제를 해결할 수 없기에 본 논문에서는 동적 사용권 관리를 통해 불법적인 사용을 근본적으로 막을 수 있도록 다음과 같은 4가지의 상품 작성 시스템을 모델로서 제시하고자 한다.

5.1 소스 수정 방식(SUM : Source Update Method)

유통 시스템이 제공하는 툴킷 이용 소스에 사용권 유무를 묻는 API를 삽입하는 방식이다. 이는 소프트웨어 상품 작성의 중요한 방식 중의 하나라고 할 수 있다. (그림 3)에서 볼 수 있듯이 다음과 같은 작업들이 저작사에 의해 수행된다. 첫째, 상품을 소프트웨어 DLC 서버에 등록한 후 등록 번호를 부여받는다. 둘째, 상품 소스에 부여된 등록 번호에 대한 사용권 유무를 묻는 API를 삽입한다. 이때 유통 시스템이 API가 포함된 툴킷을 제공한다. 이 결과 공개 상품 수행 모듈이 만들어진다. 셋째, 기타 필요한 상품 부품 및 안내서, 라이브러리 등을 함께 포함한 완성 프로그램(Packaging program 수행)으로 공개 상품을 만든다. 넷째, 완성된 상품을 여러 방법을 통해 불특정 다수에게 배포한다.



(그림 3) 소스 수정 방식의 상품 작성

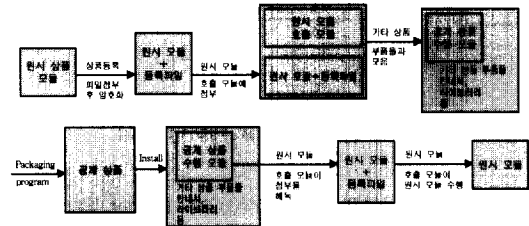
여기서 사용되는 API의 종류는 다음과 같다. 사용권 유무를 확인하는 API, 사용권 확인 API, 사용자수 문의 API, 사용자 정보 문의 API - 예를 들면, 나이조희 (미성년 여부), 학생 여부 - 등이 있다.

상품을 수행하고자 하면 상품 내에 있는 API를 통해 사용권 관리 프로그램에게 사용권 이 있는 지의 여부를 묻는다. 이때 사용권이 없고 구매를 원하면 사용권 관리 프로그램은 구매를 안내한다. 만약 사용권이 없고 구매할 의사가 없는 경우에는 사용권 관리 프로그램이 사용권이 없다고 상품에게 통보하는 즉시 상품의 수행이 중지된다.

5.2 수행 모듈 수정 방식(MCM : Module Control Module)

(그림 4)는 저작사가 완성한 원시 수행 모듈을 암호화 한 다음 유통 시스템이 제공하는 수행 프로그램에 삽입시키는 방식이다. 이 방식은 현재 한국 내에 소스를 가지지 않은 채 유통만이 이루어지는 상품들을 참여시키는데 주로 사용될 수 있으며 이것은 소프트웨어 상품

작성에 있어 보조적으로 사용되는 방식이다. 이의 과정을 간단히 살펴보면 첫째, 상품을 소프트웨어 DLC 서버에 등록한 후 등록 파일을 수령한다. 둘째, 원시 상품 수행 모듈에 등록 파일을 합한 후 암호화한다. 셋째, 유통 시스템이 제공하는 수행 모듈에 첨부한다. 이 결과 공개 상품 수행 모듈이 만들어진다. 넷째, 공개 상품 수행 모듈을 이용하여 상품을 완성(Packaging program 수행)하게 되는데 그 결과 공개 상품이 만들어진다. 다섯째, 완성된 공개 상품을 불특정 다수에게 여러 방법을 이용하여 배포한다. 여섯째, 상품 수행 시에 공개 상품 수행 모듈 내의 유통시스템 제공 수행 모듈(DPEM : DLC Provided Execution Module of Product Executables)이 첨부된 부분(원시 상품 + 등록 파일)을 해독한 후 등록 파일 정보를 이용해서 사용권을 확인한다. 일곱째, 사용권이 있으면 상품내의 원시 수행 모듈(EMOP : Execution Module of Original Product)을 수행시킨다.



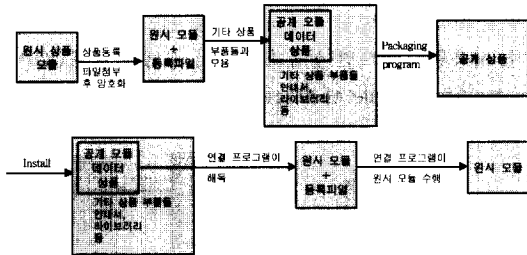
(그림 4) 수행 모듈 수정 방식의 상품 작성

5.3 수행 모듈 데이터 방식(MDM : Module Datarization Module)

(그림 5)는 저작사가 완성한 원시 수행 모듈을 데이터화하여 공개 상품으로 배포하므로 상품이 수행 가능한 형태가 아니기 때문에 사용자 PC에서 더블 클릭하면 연결 프로그램이 수행을 시켜주는 방식이다. 수행 모듈 수정 방식에서 유통 시스템이 제공하는 수행 프로그램이 사용자 PC에서 연결 프로그램으로 동작하는 방식이다. 이 방식은 디지털 데이터 상품의 처리 절차와 같아서 모든 디지털 상품 유통을 통일시킬 수 있다는 장점을 가지고 있다. 그러나 수행 모듈을 데이터화 하였으므로 단축 아이콘 작성이 불가능하다는 등의 문제점이 있을 수 있다. 이에 대해서는 앞으로 연구가 필요한 부분이라고 생각된다.

따라서 현재로서는 이 방식이 소프트웨어 상품 작성에 실험적으로만 사용되는 방식이라 할 수 있다. 이

방식의 절차에 대해 살펴보면 첫째, 상품을 DLC 서버에 등록 후 등록 파일을 수령한다. 둘째, 상품 수행 모듈에 등록 파일을 합한 후 암호화한다. 이 결과 공개 상품 수행 모듈이 된다. 셋째, 공개 상품 수행 모듈 데이터로 공개 상품을 완성한다. (Packaging program 수행) 넷째, 공개 상품을 불특정 다수에게 여러 방법으로 배포한다. 다섯째, 상품을 더블 클릭하면 연결 프로그램이 불러져 상품을 해독한다. 여섯째, 연결 프로그램으로 불러진 유통시스템 제공 수행 모듈(DPEM)이 상품을 해독한 후 등록 파일 정보를 이용하여 사용권을 확인한다. 일곱째, 사용권이 있으면 원시 수행 모듈을 수행시킨다.

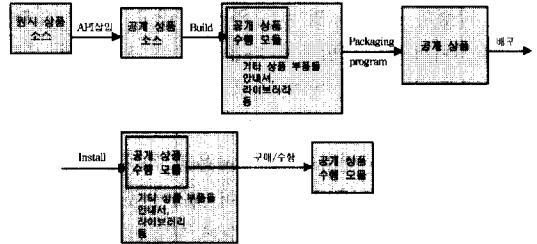


(그림 5) 수행 모듈 데이터 방식

5.4 Loader 사용권 관리 방식(LCM : Loader license Control Method)

이 방식은 (그림 6)과 같이 상품의 등록 정보를 API를 이용하여 소스에 삽입한다. 사용자가 이 상품을 수행하려고 하면 프로그램 로더가 수행 모듈 내의 상품 정보를 찾아 사용권 정보와 비교하여 실제 로드 가능 여부를 결정한다. 이 경우는 운영체제(프로그램 로더) 개발팀의 참여가 필요하다. 또한 수행 모듈의 상품 정보 해킹을 방지하기 위해 모든 모듈에 디지털 사인을 하는 것이 필요하다. 모듈에 대한 디지털 사인은 바이러스 방지라는 다른 목적을 위해서도 더 심각하게 적용이 고려되어야 하는 방법이다. 상품 정보에 대해 해킹이 되지 않았으므로 가장 바람직한 방식이지만 운영체제 개발 팀 및 컴파일러 개발 팀의 참여가 요구된다. 또한 상품정보에 대해 해킹이 되지 않았는가에 대한 검사는 저작사도 완벽하게 수행할 수 있다. 소스 수정 방식은 사용권 관리 프로그램을 호출하기 위해서 API를 사용하지만 로더 사용권 관리 방식의 경우에는 자신의 모듈 내에 일정한 형태의 상품 식별 정보를 삽입하기 위하여 API가 사용된다. 이것이 궁극적으로 가장

바람직한 방식이지만 운영체제 개발팀 및 컴파일러 개발 팀의 참여가 요구된다.



(그림 6) Loader 사용권 관리 방식

5.5 상품 작성 및 수행 방법 비교

현재는 소스 수정방식을 주로 적용하고 궁극적으로는 프로그램 Loader사용권 관리방식을 적용하여야 할 것으로 생각된다. 프로그램 로더 사용권 관리 방식은 좀더 효율적인 방법이라고 생각되지만 그 장점에 비해 많은 노력이 요구되므로 실제 적용에는 장기간이 소요될 것이다. <표 2>는 기존의 방식과 본 논문에서 소개된 방식들과를 비교한 것을 요약하였다.

<표 2> 상품 작성 방법별 비교표

| | 기존 방식 | 소스 수정 방식 | 수행 모듈 수정 방식 | 수행 모듈 데이터 방식 | Loader 사용권 관리 방식 |
|--------------|-------------|-------------------|----------------------------|---------------------------|------------------------------------|
| 상품 수정 부분 | 없음 | 상품 소스 | 수행 모듈의 암호화 | 수행 모듈의 데이터화 | 수행 모듈의 데이터화 |
| 상품 작성자 | 저작사 | 저작사 | S.O.Shop | S.O.Shop | S.O.Shop |
| 연결 프로그램 프로그램 | 없음 | 없음 | 없음 | DPEM | 프로그램 Loader |
| 상품 수행 방법 | 실행 프로그램의 수행 | 실행프로그램의 수행 | 실행 모듈(DPEM+ 암호화된 수행모듈)을 수행 | DPEM이 데이터화된 수행모듈을 수행 | 프로그램 Loader가 수행프로그램을 수행 |
| 제공 API | 없음 | 소스 수정용 API | 없음 | 없음 | 없음 |
| 안전성 | 불법복제 가능 | 안전 | 안전 | 안전 | 안전 |
| 현재 구현 여부 | O | O | O | X | X |
| 장 점 | 쉬움 | 가장 구현이 쉽고 일반적 | 소스 없는 제품 참여 가능 | 모든 디지털 상품에 동일한 처리방법 적용 가능 | 궁극적인 방법, 모든 디지털 상품에 동일한 처리방법 적용 가능 |
| 단 점 | 불법복제 가능 | 소스가 있는 제품만이 참여 가능 | S.O.Shop의 참여 준비 작업이 큼 | S.O.Shop의 참여 준비 작업이 큼 | 운영 체제 개발팀의 협력 필요 |

6. 소프트웨어 유통 시스템 구현

앞에서 설계된 소프트웨어 유통 시스템은 윈도우즈 (NT와 95/98)과 DB2 기반하에 구현이 되었다 이 시스템은 이름은 Software Online Shop(S.O.Shop)이며 현재 2개 디지털 상품(소프트웨어와 MP3)을 지원하고 있다. 이 S.O.Shop은 3개의 부분으로 이루어져 있다. 첫째는 S.O.Shop 서버이며 이는 국가 당 보통 한 개가 설치되게 된다. 이 서버는 windows NT 및 DB2상에서 구현되었다. 이곳에서 모든 상품 등록이 이루어진다. 또한 사용권을 신청한 사용자에게 해당 상품의 사용권을 인정하는 사용권 파일이 만들어지고 사용자에게 전송된다. 둘째는 S.O.Shop 클라이언트이며 이는 모든 사용자의 시스템에 설치된다. S.O.Shop Client가 설치될수 있는 환경은 windows NT, 95, 98이며 현재 Mac, Linux, Unix 및 기타 중대형 시스템에서는 설치될 수 없으나 2001년까지는 모든 플랫폼에 대한 지원 계획을 가지고 있다. 이 S.O.Shop Client는 상품의 수행 시에 사용권의 유무를 확인하게 되며 사용권이 있으면 사용권이 있다고 통보하여 계속 수행이 되도록 하지만 없을 시에는 그 즉시 수행을 중지시킨다. 셋째 S.O.Shop 저작사용 Toolkit으로서 이는 저작사가 자신들의 상품인 소프트웨어의 소스에 S.O.Shop용 API를 삽입하는데 사용된다. 이것은 저작사의 소프트웨어 상품이 개발된 환경의 컴파일러의 종류마다 다른 툴킷이 제공된다. 수행 모듈 수정 방식에서는 이 작업이 S.O.Shop측에서 이루어지고 있어 별도의 저작사용 툴킷은 제공되지 않는다.

현재 4가지 상품 작성 방법 중 실제 운용 중인 방법은 소스 수정 방식과 수행 모듈 수정방식이다. 이중 소스 수정방식은 상품 작성을 소스를 가지고 있는 저작사가 진행하게 되며 수행 모듈 수정 방식은 유통 시스템을 제공하는 측에서 상품을 작성하고 있다. 현재 운용되는 소프트웨어 상품의 거의 대부분은 소스 수정방식을 적용하고 있고 국내의 상품 보유 회사가 소스를 가지고 있지 않은 경우에만 보조적으로 수행모듈 수정방식이 이용되고 있다.

상품의 소스를 외국이 가지고 있어 모듈 수정 방식이 반드시 사용되어야 하는 경우는 DLC 유통이 좀 더 활성화되면 극히 드물게 되어 소스 수정방식만으로도 모든 상품 작성이 가능하리라고 생각된다. 현재 이 두 가지 방법만으로도 불편함이 없으나 다른 디지털 상품

의 유통과 관련지어서는 여러 가지 개선 방안들이 추 가될 수 있을 것이다.

S.O.Shop은 현재 사용자들의 가장 일반적인 상황을 전제로 동작이 된다. 사용자의 일반적인 환경은 인터넷에 원하면 연결이 될 수 있지만 항상 연결되어 있지는 않은 환경이다. S.O.Shop이 사용권 관리란 기본적으로 PC 자체 내에서 일어나며 사용자는 사용권 관리를 위해 항상 인터넷에 연결되어 있을 필요는 없다. 인터넷과 연결이 되어 있어야 하는 때는 사용자 등록, 사용권 구매 등이다.

S.O.Shop은 크게 4가지 기능 - 일반관리, 소프트웨어 관리, 음악 관리와 잔액관리 기능을 가지고 있다. S.O.Shop이 제공하는 상세한 기능들은 다음과 같다[2].

● 사용권

일정기간 사용권, 영구 사용권, 무료 사용권, 1인 사용권, 다수 사용권, 직원 사용권 등을 지원한다.

다수 사용권은 5인용 NT사용권의 경우처럼 허용 사용자수에 따라 가격을 다르게 지불하고 허용되는 사용자수 만큼만 사용할 수 있게 하는 구조를 제공하는 것이다. 직원 사용권은 어느 회사가 개발한 제품을 그 회사 직원도 구매하여야만 사용할 수 있는 상황을 막기위해 자기회사 직원의 경우 무료 사용이 가능한 구조를 제공한다.

● 가격 - 일반 가격, 학생가격, 신규 구매 가격, 업그레이드 구매 가격, 사용자수별 가격이 적용된다. 이 가격들은 신분증 정보 및 기존 사용권 정보에 의해 자동 적용이 된다.

● 일반 사용자 기능 - 사용자 정보 조회, 사용자 정보 변경, 신분증 갱신, 신분증 복구, 사용권 복구 구매 기능, 음악 선물, 사용권 정보 보기, 선물권 구매, 음악 구매, 소프트웨어 구매, 잔액조회 등의 기능이 있다.

● 법인 사용자 기능 - 소프트웨어 자산 목록(회사별 전체 소유 소프트웨어 목록을 조회할 수 있는 기능) 퇴직자 처리 기능(퇴직자의 소프트웨어를 다른 직원이 사용할 수 있게 반납 가능)

● 상품 생산자 기능 - 소프트웨어 기증, 소프트웨어 상품 등록, 음악 상품 등록, 소프트웨어 판매 보고서 음악 판매 보고서

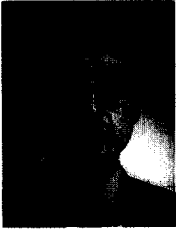
7. 결론 및 향후 연구 과제

본 논문에서는 동적 사용권 관리 시스템을 이용하여 전자상거래 시대에 있어서 디지털 소프트웨어 상품의 안전하고도 편리한 유통 구조를 구축할 수 있음을 제시하였다. 즉, 동적인 사용권 관리 방법을 통해 첫째, 디지털 소프트웨어 상품의 유통을 위한 요구사항을 살펴보고 둘째, 디지털 소프트웨어 상품의 불법 재생 및 배포를 차단할 수 있는 유통 구조를 제시하였으며 셋째, 디지털 소프트웨어 상품 작성 모델들을 제시하여 유통의 안전성을 확대할 수 있는 방법을 제시하였으며 넷째, 이 모델 중 실제 구현한 사례를 소개하였다.

앞으로 전자상거래에 있어 중요한 요소인 인증기관과의 통합을 통해 동적 사용권 관리 서버에서의 회원 가입 단계를 생략하는 것, OS와의 번들을 통해 사용권 관리 사용자 프로그램의 설치를 생략하는 것, 제품 배포 수단의 강화, 해킹 방지 방안 연구, 워터마크의 강화 등은 기반 환경 요소라 할 수 있는 지분 시스템의 향상, 네트워크 스피드의 향상 등과 함께 개선되고 연구되어야 할 과제라 할 수 있다.

참 고 문 헌

- [1] 강우준, 김용모, "디지털 상품의 온라인 유통을 위한 동적 사용권 관리 기술", 한국정보처리학회 춘계 학술 발표 논문집, 제7권 제1호, 2000.
- [2] 박효준, 강우준, "세계 디지털 상품 유통 기술의 동향과 S.O.Shop", 한국정보처리학회 학회지, 제7권 제2호, 2000.
- [3] W. Diffie and M. E. Hellman, "New Directions in cryptography," IEEE Trans. on Information Theory IT-22 No.6, pp.644-654, 1976.
- [4] R. L. Rivest, A. Shamir and L. Adleman, "A method of obtaining digital signature and public key cryptosystem," ACM Communication, 21 No.2, pp. 120-126, 1978.
- [5] 원동호, "암호 방식과 키분배", 한국통신정보보호학회 학회지, 제1권 제1호, pp.72-82, 1991.
- [6] 손기욱, 이윤호, 권창영, 원동호, "ID 정보에 의한 암호키 분배 방식", 정보보호와 암호에 관한 워크샵 논문집, pp.129-141, 1991.
- [7] 임채훈, 이필중, "상호신분 인증 및 디지털 서명기법에 관한 연구", 한국통신정보보호학회 논문집, Vol. 2, No.1, pp.16-35, 1992.
- [8] 염홍렬, "디지털 서명 방식 고찰", 한국통신정보보호학회 학회지, 제3권 제2호, pp.7-18, 1993.
- [9] YeonYi Choi, SeungJoo Kim, SungJun Park and DongHo Won, "A paradoxical ID-based key distribution protocol for mobile communication systems," KITE, IXICE and IEEE, pp.412-415, 1996.
- [10] 임신영 외, "디지털 지적 재산권 보호를 위한 인증 응용 기술", EC/CALS 기술 워크샵 발표자료집, pp. 271-275, 1999.
- [11] 임신영 외, "디지털 상품의 유통 정보 관리 기술", 한국전자거래학회/한국정보시스템학회 종합학술대회 논문집, pp.373-384, 1999.
- [12] 윤우성 외, "DLC를 이용한 디지털 데이터의 불법 복제 방지 시스템 연구", 한국정보처리 학회 추계 학술 발표 논문집, 제6권 제2호, 1999.
- [13] 강상승 외, "MP3 미디어 데이터의 온라인 유통 기술", 한국전자거래학회/한국정보시스템학회 종합학술대회 논문집, pp.589-600, 1999.
- [14] IBM, ESD(Electronic Software Distribution), URL : <http://www.spa.org/signs/internetesdpoli.htm>
- [15] Mars System Inc., DLC(Dynamic License Control), URL : <http://www.soshop.co.kr/>
- [16] 이광수, "Digital Watermarking 방법을 이용한 디지털 미디어 콘텐츠의 Copyright 보호 방법", URL : <http://monami.kaist.ac.kr/~guspin/report/cs540/watermark.html>
- [17] SDMI "Identifies Audio Watermark Technology for Next Generation Portable Devices for Digital Music," URL : http://www.sdmi.org/pr/NY_Aug_9_1999_PR.htm



강 우 준

e-mail : wjkang@ansantc.ac.kr

1984년 연세대학교 전자공학과
(공학사)

1984년 한국 IBM S/W 연구소

1991년 한국 IBM S/W 연구소
의료정보시스템 개발 팀장

1992년 연세대학교 전자계산학
(공학 석사)

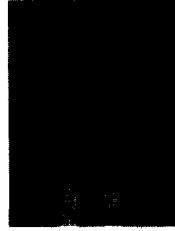
1994년 연세대학교 경영정보학(경영학 석사)

1998년 한국 IBM S/W 연구소 EDMS 개발 담당 부장

1999년 성균관대학교 전기전자 및 컴퓨터 공학부 박사
과정 수료

1999년~현재 안산공과대학 전산정보과 교수

관심분야 : 사용권관리, 전자상거래, 데이터베이스, 지식
관리시스템, 의료정보시스템



김 응 모

e-mail : umkim@yurim.skku.ac.kr

1981년 성균관대학교(이학사)

1986년 미국 Old Dominion

University(이학석사)

1990년 미국 Northwestern

University(이학박사)

1998년 정보통신연구관리단 선정평가위원

현재 성균관대학교 전기전자 및 컴퓨터 공학부 교수

1999년~현재 정보처리학회 편집부위원장