

저작권 위탁 관리를 위한 P-ESD (Protection-ESD) 시스템 설계

박복녕, 김정범, 김태운
고려대학교 컴퓨터학과
e-mail : happy@netlab.korea.ac.kr

Design of P-ESD(Protection-ESD) System for Copyright Trusty Management

Bok-Nyong Park, Jeong-Beom Kim, Tai-Yun Kim
Dept of Computer Science & Engineering, Korea University

요약

전자 상거래의 발전과 더불어 디지털화된 모든 콘텐츠는 인터넷을 통해 배포되어 이용되고 있다. 소프트웨어도 예외는 아니어서 기존에 오프라인을 통해 유통되던 소프트웨어들이 ESD(Electronic software Distribution)를 통해 온라인으로 유통되고 있다. 그러나 기존의 ESD 모델들은 소프트웨어의 불법복제문제를 해결하지 못하고 저작권보호에 미흡하다는 단점이 있다. 이에 본 논문에서는 ESD에 DRM기술을 사용하여 소프트웨어의 불법사용방지와 다양한 사용권한 제어가 가능한 P-ESD(Protection-ESD) 메커니즘을 제안한다. 제안한 모델은 불법사용을 방지하여 소프트웨어 저작권을 보호하고 다양한 지불방법을 제공한다.

1. 서론

인터넷을 통한 전자상거래는 실생활의 상거래보다 편리함과 효율성을 가지고 있어서 사용자 수가 급증하고 있다. 이러한 전자상거래 유통 시장이 성장하면서 기존에 오프라인을 통해 유통되던 소프트웨어들이 ESD를 통해 온라인으로 유통이 되고 있다.

ESD(Electronic Software Distribution)란 온라인을 통해 소프트웨어 제품의 전자적 구매 및 배송이 가능한 시스템 구성 요소를 말한다[1]. 현재 인터넷 상에서 적지 않은 온라인 쇼핑몰들이 소프트웨어의 다운로드 서비스를 하고 있다. ESD는 인터넷을 통해 소프트웨어의 판매 및 배송이 이루어지기 때문에 시간과 공간의 제약이 없을 뿐만 아니라 상품 포장비나 유통비를 크게 줄일 수 있다. 소비자의 입장에서 보면 구매가 간편하고, 구매 즉시 사용할 수 있을 뿐만 아니라 일반적인 패키지 상품가격 보다 저렴한 가격에 소프트웨어를 구입할 수 있다는 장점이 있다. 그러나 소프트웨어는 복제가 용이하고 복사본이 원본과 동일하기 때문에 인터넷을 통한 소프트웨어의 대량불법 복제와 유통이 이루어질 수 있다는 단

점이 있다. 또한 인터넷은 불완전한 개방형 네트워크이기 때문에 개인의 정보보호에 취약하다는 문제점이 있다. 따라서 사용자가 원하는 다양한 지불 방법을 충족하고 동시에 소프트웨어의 불법 복제 및 유통을 방지하는 새로운 방법이 필요하다.

본 논문에서는 기존의 ESD에 디지털 콘텐츠의 저작권 보호 기술로 알려진 DRM(Digital Rights Management)기술의 개념을 도입하여 소프트웨어의 불법사용방지와 다양한 사용권한 제어를 가능케하는 P-ESD(Protection-Electronic Software Distribution) 메커니즘을 제안한다. 논문에서 제안하는 P-ESD는 기존의 ESD에 보호기능을 부가하여 소프트웨어의 불법 사용을 방지하고 다양한 지불 방법을 제공한다.

본 논문의 2장에서는 현재 사용하고 있는 ESD 모델들에 관하여 분석하고 DRM 기술에 대해 알아본다. 3장에서는 제안한 P-ESD를 설계한다. 4장에서는 기존의 ESD 모델들과 제안한 모델을 비교 분석하고 5장에서 결론을 맺는다.

2. 관련 연구

2.1 ESD 모델

ESD는 온라인을 통해 소프트웨어 제품의 전자적 구매 및 배송이 가능한 시스템 구성 요소를 일컫는 기술적 의미와 전자적인 소프트웨어 유통을 위해 필요한 유통구조와 판매 기법 등 유통 환경 전반을 포함하는 마케팅적 의미로 받아들여지고 있다. 그림 1은 ESD 모델의 유통 과정이다[3].

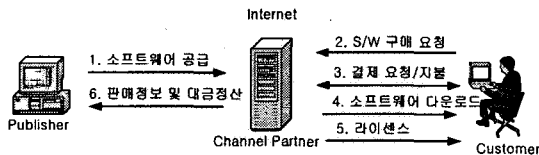


그림 1 ESD 모델

ESD 모델에는 선지불(Buy-first) 방법, 후지불(Try-before-buy) 방법, 그리고 전자 사용권(EL : Electronic License) 방법이 있다.

선지불 방법은 기존의 오프 라인 환경에서의 소프트웨어 판매 방법을 전자상거래 환경에 적용한 방법으로 사용자가 상품을 선택하고 상품의 가격을 먼저 지불한 후 소프트웨어를 설치하는 방법이다. 선지불 방법을 적용한 소프트웨어 분배 시스템은 Preview Systems사의 집락(ZipLock) 시스템을 예로 들 수 있다[4]. 선지불 방법은 구매 절차가 간단하나 사용자는 소프트웨어를 구매하기 전에는 소프트웨어에 대한 자신의 만족도를 평가할 수 없으며 네트워크 상에서 키가 다른 이에게 노출되거나 사용자가 악의를 품는 경우 불법 복제 및 유통을 막을 수 없다.

후지불 방법은 구입하고자 하는 소프트웨어를 사용한 후 구입 여부를 결정하는 시스템으로 판매자는 날짜에 기초하여 상용기간에 제한을 둔 소프트웨어나 기능에 제한을 둔 시범 소프트웨어를 제공한다. 후지불 방법을 적용한 소프트웨어 분배 시스템은 Preview Systems사의 브릭스(Vbox) 시스템이 있다[4]. 후지불 방법을 이용한 판매 방식은 선지불 방법보다 사용자의 만족이 높지만, 구매 절차가 복잡하고 잠금 장치를 해제한 소프트웨어의 불법 복제 및 유통을 방지할 수 없다.

선지불 방법과 후지불 방법은 전자상거래가 가지고 있는 이점을 그대로 가지고 있다고 하겠다. 그러나 전자상거래에서 보장되어야 할 보호가 미흡하다. 전자 사용권 방법은 이를 좀더 개선하여 제안된 방법이다. 이 모델은 소프트웨어의 사용권을 제품으로부터 분리시킨 후 사용권을 판매하는 시스템으로,

사용자는 원하는 소프트웨어를 즉시 다운로드 할 수 있지만 소프트웨어의 사용을 위해서는 지불과 등록을 통하여 사용권을 전달받아야 한다. 시만텍사(Symantec)에서 이 방법을 사용한 소프트웨어의 온라인 판매가 이루어지고 있다[5]. 전자 사용권 모델은 사용권을 따로 관리하므로 불법 복제 및 유통을 방지하는데 효과적이다. 그러나 다양한 종류의 소프트웨어에 대하여 사용자가 원하는 적절한 지불 방법을 제공하지는 못한다.

2.2 DRM(Digital Right Management)

DRM은 암호화 기술을 바탕으로 디지털 콘텐츠의 불법복제를 방지하며, 저작권을 보호하기 위한 하드웨어와 소프트웨어를 포함한 포괄적인 저작권 관리 기술이다. 그림 2는 DRM 모델을 보인다[7].

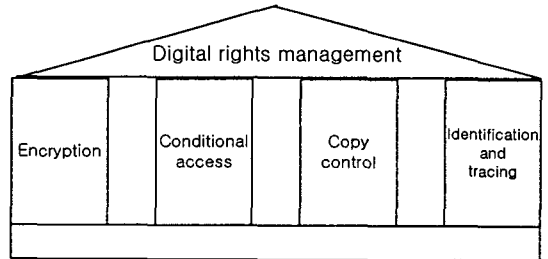


그림 2 DRM 모델

DRM이 제공하는 주요 요소 기술은 다음과 같다.

- 변조 방지 소프트웨어 : DRM 시스템에 대한 공격의 대부분이 사용자 모듈에서 발생한다. TRS (Tamper Resistant Software)는 DRM 클라이언트 모듈에 대한 공격으로부터 콘텐츠를 보호하는 핵심 기술로 Microsoft, Intertrust 등 세계의 일부 주요 DRM 업체에서 TRS 기술을 개발중이다.
- 암호 키와 안전한 콘텐츠 유통 : 암호 기술을 이용한 콘텐츠 보호와 키 분배 및 관리 메커니즘으로, 콘텐츠의 보호 및 사용 권한 정보 인증을 위한 암호화/서명 기술을 이용하여 컨테이너(Secure Container)형태로 가공한다.
- 공개키 기반 구조 : 안전한 키 관리와 사용자/클라이언트 소프트웨어 인증을 제공하여 전반적인 콘텐츠 분배 메커니즘이 안전하게 수행되도록 보장하는 기술로, DRM 기술간의 상호 운용성을 제공하기 위한 필수 조건이다.
- 권한 명세 언어 : 저작권, 사용권 등의 콘텐츠 관리 정보를 기술하는 XML 형식의 언어로, 현재

3-4개 정도의 권한 명세 언어에 대해 W3C, MPEG21 등에서 표준 선정 작업을 진행 중이다.

- 디지털 워터마킹 : 콘텐츠로부터 저작권 정보(저작권자, 분배자/소비자)를 삽입하여 저작권 확인, 콘텐츠 추적 정보, 재분배자 식별(fingerprining) 기술로 향후 불법 복제 발생시 사후 구제 수단을 제공한다.
- Clearinghouse : 콘텐츠의 사용권을 부여하고 이에 대한 지속적 관리를 담당하는 시스템이 필요하게 되는데 이러한 역할을 담당하는 것이 clearinghouse이다. Clearinghouse는 전송된 결제 정보 및 사용내역을 처리해서 콘텐츠 소유자와 콘텐츠 유통업자에게 정산 금액 및 판매 내역을 제공한다.
- Superdistribution : 콘텐츠 사용자는 이 콘텐츠를 다른 사용자에게 전달 할 수 있다. 비록 구매한 이용자가 콘텐츠에 대해 사용권한을 취득한 상태라고 하더라도 전달받은 사용자가 사용규정을 만족해야만 사용권한을 부여받을 수 있다.

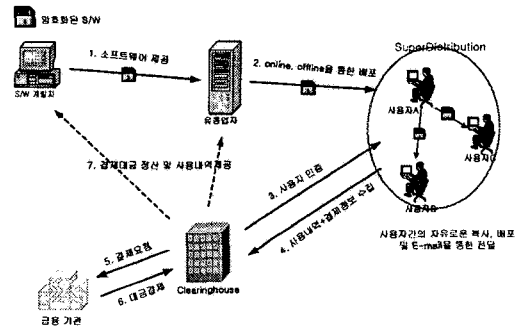


그림 3 제안한 P-ESD 모델

3. 제안한 P-ESD 모델

기존의 ESD 모델은 온라인을 통한 소프트웨어 유통을 위해 필요한 기능을 제공하고 있으나 배포된 소프트웨어의 불법 사용 방지 및 저작권에 대한 기술적 보호 조치들이 미흡한 상태에 있다. 이에 본 논문에서 제안한 P-ESD 모델은 저작권 보호를 위하여 기존의 ESD에 디지털 콘텐츠의 불법사용방지 및 저작권보호를 위해 사용되는 DRM 기술을 접목하여 설계한다.

3.1 P-ESD 시스템의 구성

제안한 P-ESD 시스템에 참가하는 주체로는 소프트웨어를 제작하여 제공하는 소프트웨어 개발자 (publisher), 소프트웨어 제공자로부터 소프트웨어를 받아 대신 분배하고 제공해주는 소프트웨어 유통업자(channel partner), 사용자(client) 그리고 소프트웨어 사용권한을 부여하고 지속적인 관리를 담당하며 사용자로부터 전송된 결제내역과 사용내역에 대한 처리를 하는 clearinghouse로 구성된다. 그림 3은 제안한 P-ESD 시스템 모델이다.

소프트웨어 개발자는 개발하여 판매하고자 하는 소프트웨어를 암호화하여 소프트웨어 유통업자에게 제공하고 판매를 위탁한다. 소프트웨어는 사용규칙

과 해당 소프트웨어의 설치 요소를 묶어 콘텐츠로 암호화한다. 소프트웨어 유통업자들은 배포하고자 하는 소프트웨어의 상품정보를 판매 사이트에 등록한다. 사용자는 유통업자의 판매 사이트에서 원하는 소프트웨어를 선택하여 다운로드 한다. 소프트웨어의 다운로드는 아무런 제약 없이 무료로 다운로드하여 배포되고 오프라인 상에서도 복제가 가능하다. 다운로드한 소프트웨어는 결제가 이루어지지 않으면 암호를 풀 수 없기 때문에 소프트웨어를 설치할 수 없다. 사용자 인증과 결제 정보를 clearinghouse가 확인한 후에 암호화된 소프트웨어를 복호할 수 있는 키를 e-mail을 통해 암호화하여 사용자에게 전송한다. 사용자는 ID와 부여받은 키를 이용하여 소프트웨어를 설치할 수 있다. Clearinghouse 사용자로부터 받은 결제 정보로 금융기관에 대금 결제를 요청하여 대금 결제를 받은 후에 서비스 개발자와 유통업자에게 결제 대금을 정산한다. 동시에 소프트웨어의 사용내역을 제공한다. 제안한 시스템에서 사용자는 자유롭게 주위사람에게 복사를 통해 소프트웨어를 배포할 수 있다. 그러나 소프트웨어를 사용하고 자 하는 사용자는 반드시 정당한 사용자 인증과 대금 결제 이후에만 소프트웨어를 설치하여 사용할 수 있다. 논문에서 clearinghouse는 소프트웨어의 결제 처리와 소프트웨어 사용 관리 및 사용자의 사용 내역들을 수집/관리하는 기능을 수행하며, 사용자 인증 기능을 가지고 있다. 또한 판매된 금액을 소프트웨어 개발업자와 소프트웨어 유통업자들에게 정산하는 업무를 담당한다.

3.2 소프트웨어 설치와 사용

암호화된 소프트웨어는 설치하여 사용하려 할 경우 ID와 복호키를 요구한다. 복호키는 사용자 인증과 대금 결제가 정상적으로 이루어지면 e-mail을 통

해 암호화하여 전송한다. 사용자는 암호화된 e-mail을 복호하여 키를 얻는다. 암호화된 소프트웨어는 인터넷에 연결된 상태에서만 설치와 삭제가 가능하다.

사용자가 ID와 키를 입력하면 소프트웨어는 설치를 위해 clearinghouse에 연결하여 사용자 인증을 받고 등록을 한다. 삭제할 경우에 clearinghouse에 다시 연결되어 설치 정보를 삭제하고 다시 다른 컴퓨터에 설치할 수 있다. 이 방법은 설치할 경우에 서버에 등록하여 인증을 받은 후 설치할 수 있기 때문에 복제가 되더라도 이미 설치가 되어있으면 서버에서 설치에 대한 등록이 되어 있으므로 서버는 소프트웨어의 복호를 거부하여 설치를 하지 못한다. 삭제의 경우도 같은 과정을 따른다. 그림 4는 소프트웨어 설치와 삭제 과정을 보인다.

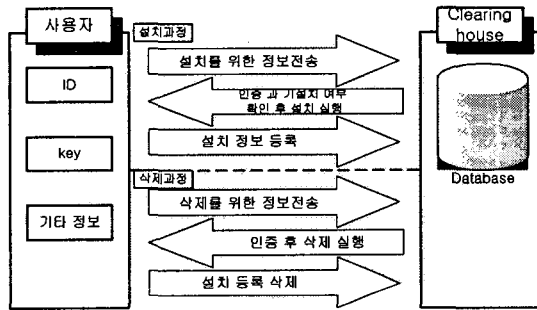


그림 4 소프트웨어 설치/삭제 과정

4. 성능 분석

표 1은 제안한 P-ESD와 기존 ESD 모델의 성능을 비교한 것이다.

표 1 제안한 모델과 다른 ESD 모델의 성능 비교

적용시스템 비교항목	집락	브이 박스	시만텍	제안한 시스템
불법 복제 방지	×	×	△	○
불법 사용 방지	×	×	△	○
Superdistribution	×	×	○	○
다양한 지불방법 지원	×	×	×	○
판매자 이익보호	○	△	○	○
네트워크 의존도	△	△	△	○

(○ : High △ : Low × : None)

집락과 브이박스는 잠금 장치를 해제한 소프트웨어에 대하여 무한한 불법 복제가 가능하다. 시만텍은 사용권을 관리하여 불법 유통을 막는 효과가 있

으나 사용자가 사용권을 다른 사람에게 나누어주는 경우 불법 복제를 막을 수 없다. 제안한 P-ESD 모델은 설치할 경우 서버에 등록하여 인증을 받은 후 설치하기 때문에 복제가 되더라도 이미 설치가 되어 있으면 서버에서 설치에 대한 등록이 되어 있으므로 서버는 설치를 거부하기 때문에 복제방지의 기능을 갖는다. 따라서 자유롭게 복사는 가능하지만 사용은 불가능하다. 또한 clearinghouse에서 결제 정보를 수집한 후 금융기관과 상호 작동을 하여 결제하므로 다양한 결제 수단을 제공할 수 있다.

5. 결론 및 향후 연구 과제

기존의 ESD 모델은 전자적인 소프트웨어 전송 방법과 판매에 치중되어 있어서 소프트웨어 불법복제와 유통 및 저작권 보호에 미흡하고 다양한 지불 방법을 해결하지 못하였다.

본 논문에서는 기존의 ESD 모델에 디지털 콘텐츠의 저작권보호 기술인 DRM을 사용하여 소프트웨어의 불법 복제를 차단해 소프트웨어 제작업자의 저작권을 보호하는 P-ESD를 제안하였다. 제안한 P-ESD 기술은 소프트웨어 저작권을 보호하고, super-distribution의 도입으로 자유로운 분배가 가능할 수 있었다. 또한 clearinghouse의 이용으로 다양한 결제를 제공할 수 있었다. 향후 연구과제로는 네트워크에 의존을 낮추고 오프라인 상에서도 저작권 보호가 보장되는 연구가 필요하다.

참고문헌

[1] ESD, <http://www.esd.com>
 [2] 김영준, 이성민, 이윤정, 박남섭, 이병래, 김태운, "소프트웨어 저작권 보호를 위한 전자 소프트웨어 유통 프로토콜의 설계", 정보과학회논문지, v.7, n.4, DECEMBER 2001.
 [3] 강호갑, "소프트웨어 저작권 보호기술", 정보화시대 저작권 소식지, 2001.
 [4] preview, <http://www.previewsystems.com>
 [5] NL, <http://www.symantec.com/region/kr>
 [6] DRM, <http://www.fasoo.com>
 [7] Hartung, Ramme, F., "Digital rights management and watermarking of multimedia content for m-commerce applications", IEEE communications Magazine Vol.38 No.11, Nov. 2000