2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

소프트웨어 온라인 판매 기술 연구

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

A Study on Software On-line Sells

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

요약

전자 상거래가 활성화되면서 네트워크를 이용한 상품의 구매가 점점 증가하고 있다. 현재 전자 상거래에 이용되는 대부분의 상품은 하드웨어가 주를 이루고 있다. 소프트웨어의 온라인 판매는 물류비용이 없고 수익성이 높은 장점을 가지고 있지만 불법 복제 문제 때문에 현재 전자 상거래에서는 기피 상품으로 취급받고 있다.

본 논문에서는 사용권 관리 기술을 이용하여 소프트웨어의 불법 복제를 막을 수 있는 소프트웨어 온라인 판매 기술을 소개한다.

1. 서론

인터넷 웹 기술로 인한 인터넷의 대중화가 시작되면서 인터넷 전자상거래가 대중화되었고, 네트워크의 고속화가 실현되면서 각종 컴퓨터 응용 소프트웨어, 멀티미디어 데이터들이 전자파일 형태로 판매가 가능하게 되었다. 소프트웨어 온라인 판매는 편리한 구매와 즉각적인 배달이 가능하다 또한, 상품 판매비용이 감소하고, 판매에 대한 효율적인 통계작업이 가능하며 상품의 업그레이드와 유지보수 관리를 쉽게 할 수 있고, 상품 관리를 위한 물리적 재고 장소가 필요 없고, 비용의 추가가 없어서 판매에 대한 유연성을 쉽게 획득할 수 있다는 장점을 가지고 있다[1].

그러나 소프트웨어는 특성상 불법 복제 및 유통이 용이하고 소요되는 비용이 전혀 없다. 따라서 기술적인 뒷받침이 없이 불법 복제 소프트웨어를 사용하지 말자는 호소성 조치로는 사용자들로 하여금 무료로 또는 저렴한 비용으로 정품 소프트웨어를 불법으로 사용할 수 있다는 유혹을 원천적으로 방지할 수 없다[2].

본 논문에서는 사용권 관리 기술을 이용하여 소프트웨어의 불법 복제를 막을 수 있는 소프트웨어 온라인 유통 기술에 관하여 소개한다. 본 논문의 구성은 2장에서는 기존의 전자 사용권 모델을 제시한다. 3장에서 소프트웨어 판매 및 관리 기술을 설명한다. 4장에서 시뮬레이션 결과를 통한 성능을 평가한다. 5장에서 결론 및 향후 연구 과제를 제시한다.

2. 전자 사용권 모델

전자 사용권 모델은 소프트웨어의 사용권을 제품으로부터 분리시킨 후 사용권을 관리하는 시스템이다. 전자 사용권 모델에서 사용자는 원하는 소프트웨어를 즉시 다운로드 할 수 있다. 하지만 어떤 소프트웨어 제품이 PC상에 설치되어 있더라도 사용권이 없으면 수행되지 않기 때문에 소프트웨어의 사용을 위해서는 지불과 등록을 통하여 사용권을 전달받아야 한다. 이 모델에서는 소프트웨어가 실행될 때 현재 사용자가 제품의 사용권이 있는지 확인하고 확인 결과에 따라 소프트웨어가 계속 작동하던가 작동이 중지되거나 하기 때문이다[3]. 시맨텍사(Symantec)에서는 전자 사용권 모델을 적용한 소프트웨어의 온라인 판매가 이루어지고 있다[4]. 그림 1은 전자 사용권 모델을 이용한 소프트웨어 구매 절차이다. 전자 사용권 모델은 사용권을 따로 관리하

므로 불법 복제와 불법 유통을 방지하는데 효과가 있다고 할 수 있으나 사용자가 자신의 사용권을 불법으로 유통시키는 것을 막을 수 없다.

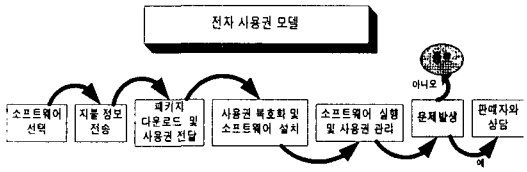

그림 1 전자 사용권 모델

3. 소프트웨어 판매 및 관리

3.1 소프트웨어 구매

소프트웨어 구매 절차에서 첫 번째 수행되는 과정은 사용자가 판매자 시스템에서 소프트웨어 패키지와 사용권을 전달받는 것이다. 사용자는 판매자의 홈페이지를 통하여 원하는 소프트웨어를 선택 할 수 있다. 판매자는 먼저 사용자를 인증하여야 한다. 판매자가 사용자들을 회원으로서 관리하면 소프트웨어 구매시 별도의 인증 절차를 거치지 않아도 된다. 인증 받은 사용자는 판매자가 제작한 소프트웨어 패키지를 다운로드 할 수 있다.

본 시스템에서는 판매자가 사용권을 암호화하여 사용자에게 전자 메일로 전달한다. 공개키 기반 구조[5]를 가정하므로 판매자는 사용자 공개키(P_{user})와 판매자 비밀키(S_{seller})를 가지고 있다. 사용자도 판매자 공개키(P_{seller})와 사용자 비밀키(S_{user})를 가지고 있다. 판매자 시스템에서는 생성한 사용권을 사용자 시스템에서만 사용할 수 있게 하기 위하여 P_{user}로 암호화한다. 판매자 시스템은 이것을 다시 S_{seller}를 이용하여 전자 서명한다. 판매자가 사용자에게 보내는 암호화된 사용권은 다음과 같다.

$$\text{암호화된 사용권} = S_{seller}(P_{user}(\text{사용권}))$$

3.2 사용권 관리 프로그램과 소프트웨어의 설치

사용권 관리 프로그램은 암호화된 사용권을 이용하여 사용자와 설치하려는 소프트웨어를 인증한다. 사용자는 판매자의 비밀키를 모르기 때문에 암호화된 사용권을 생성할 수 없다. 사용자가 사용권을 조작하는 것을 방지하기 위하여 사용권 관리 프로그램은 암호화된 사용권을 전달받는다. 사용권 관리 프로그램은 암호화된 사용권을 복호화하기 위하여 사용자 시스템으로부터 사용자 비밀키를 전달받는다. 사용자의 비밀키는 절대 외부에 공개되어서는 안되기 때문에, 사용권 관리 프로그램은 판매자 시스템에서 데몬(Daemon) 프로세스로 실행되고, 사용자 시스템은 루프백 어드레스(127.0.0.1)를 이용하여 사용권 관리 프로그램에게 데이터를 전달한다. 사용자 시스템에 사용권 관리 프로그램과 소프트웨어 설치 절차는 그림 2와 같다.

① 사용자는 판매자 홈페이지에서 사용자 인증을 확인 받고, 사용자 ID를 발급 받는다. 소프트웨어 관리에 필요한 소프트웨어 관리 프로그램을 다운로드 받는다.

② 사용자 ID를 입력하기만 하면 소프트웨어 관리 프로그램은 설치 완료된다. 소프트웨어 관리 프로그램은 소프트웨어 ID를 이용하여 각각의 소프트웨어를 관리하므로 사용자 시스템에 한번만 설치하면 된다.

③ 사용자는 원하는 상품을 선택하고 사용권 제작에 필요한 정보를 입력한다. 사용자는 홈페이지를 통하여 소프트웨어 패키지를 다운로드하고, 암호화된 사용권을 전자 메일로 전달받는다.

④ 소프트웨어를 설치하기 위하여 사용자 ID를 입력한다. 이 사용자 ID는 ⑥번 과정에서 소프트웨어 관리 프로그램이 가지고 있는 사용자 ID비교함으로서 소프트웨어를 설치하려는 사람이 정당한 사용자임을 인증 하는데 사용된다.

⑤ 소프트웨어 패키지는 사용자로부터 전달받은 사용자 ID와 판매자가 기록한 소프트웨어 ID를 사용권 관리 프로그램에게 전달한다. 이 소프트웨어 ID는 ⑥번 과정에서 사용권으로부터 가져온 소프트웨어 ID를 비교하여 소프트웨어를 인증한다.

⑥ 소프트웨어 관리 프로그램은 사용자가 입력한 암호화된 사용권을 복호화하고 사용자 ID와 소프트웨어 ID를 이용하여 사용자와 소프트웨어 패키지를 인증한다.

⑦ 소프트웨어 관리 프로그램은 인증 결과를 소프트웨어 패키지에게 전달하고 인증 결과가 OK이면 소프트웨어 설치를 수행한다.

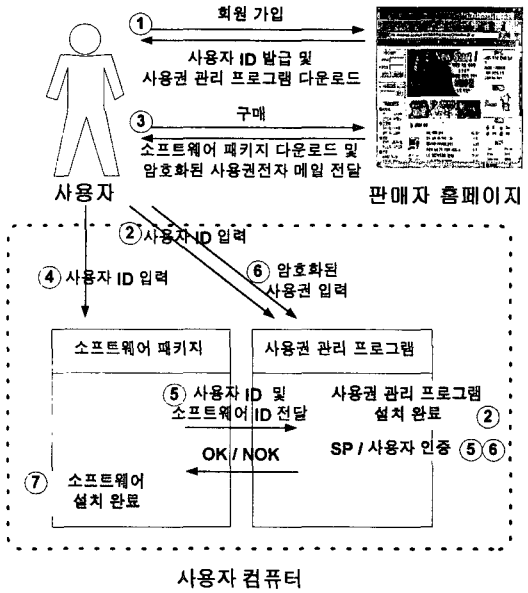

그림 2 소프트웨어 설치 절차

3.3 소프트웨어 실행과 사용권 관리

사용권 관리 프로그램은 소프트웨어 실행시 소프트웨어의 정품 여부를 인증하여 소프트웨어를 관리한다. 사용권 관리 프로그램은 암호화된 사용권을 복호화 하여 사용권 정보를 메모리에 기억하고 있다. 사용자가 소프트웨어 실행시 소프트웨어는 소프트웨어 ID라는 것을 사용권 관리 프로그램에 전달하는데, 사용권 관리 프로그램이 이것을 사용권 정보에서 가져와 비교하여 소프트웨어를 인증하는 것이다. 만일 현재 실행하고 있는 소프트웨어의 ID가 잘못 되거나 누락되어 있는 경우 사용권 관리 프로그램이 이것을 강제 종료시키게 되므로, 사용자가 불법으로 소프트웨어를 배포한다 하더라도 사용권 관리 프로그램의 인증이 없다면 소프트웨어를 사용할 수 없다. 그림 3은 소프트웨어 관리 절차를 나타내었다.

① 사용자는 자신이 구매한 암호화된 소프트웨어 사용권을 사용권 관리 프로그램에게 전달한다. 사용권 관리 프로그램은 이를 복호화하여 메모리에 올려 놓는다.

② 소프트웨어는 실행시 소프트웨어 ID를 사용권 관리 프로그램에 전달한다. 만일 전달하지 못한다면 소프트웨어는 실행되지 않는다.

③ 사용권 관리 프로그램은 전달 받은 소프트웨어 ID와 사용권에 적혀 있는 소프트웨어 ID와 비교한다. 만일 일치하게 되면 소프트웨어를 인증하는 것으로 사용자는 무리 없이 소프트웨어를 사용할 수 있다.

④ 사용권 관리 프로그램에서 소프트웨어 ID에 해당하는 사용권을 찾지 못하는 경우 이것은 사용권이 존재하지 않는 불법 복제된 소프트웨어로 간주하여 NOK 메시지를 전달하는 동시에 소프트웨어 프로세서를 강제 종료시킨다.

⑤ NOK 메시지를 전달받은 소프트웨어는 작업이 강제 종료된다.

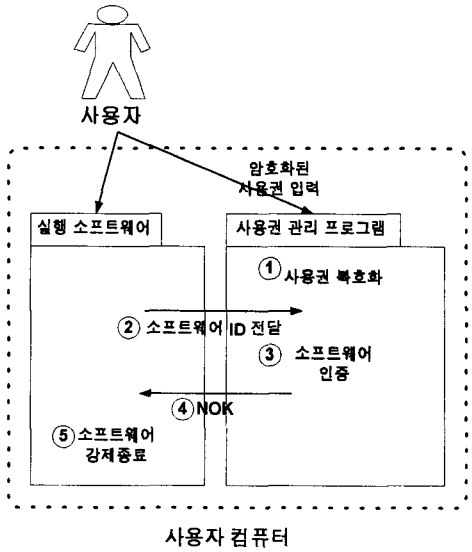

그림 3 소프트웨어 관리 절차

4. 성능 평가

본 시스템은 암호 알고리즘을 이용하여 메시지를 교환하므로 메시지의 무결성이 보장된다. 전자 사용권 모델은 불법 유통을 막는 효과가 있으나 사용자가 사용권을 다른 사람에게 나누어주는 경우 불법 복제를 막을 수 없다. 제안한 시스템은 공개키 기반 암호 알고리즘을 이용하여 암호화된 사용권을 전달한다. 사용자는 판매자의 공개키(P_{seller})와 자신의 비밀키(S_{user})를 이용하여 평문의 사용권을 얻을 수 있고 조작이 가능하다. 그러나 사용권을 인증하는 사용권 관리 프로그램은 암호화된 사용권을 복호화하여 사용한다. 따라서 사용자가 사용권을 불법 복제하여 배포하더라도, 사용자들은 판매자의 비밀키를 모르기 때문에 불법 복제된 사용권으로부터 암호화된 사용권을 만들 수 없다. 따라서 제안한 시스템은

불법 복제 방지 효과가 크다.

표 1은 512 비트의 데이터를 RSA[6] 알고리즘을 이용하여 본 시스템에서 사용하는 사용권 관리 프로그램에서 암호화된 사용권을 복호화하여 데이터를 얻어내는데 소요된 시간을 측정한 것이다. 표 1의 결과에 따르면 소프트웨어 시작전 사용권 획득시간이 0.3초가 소요된다. 그러나 이것은 시스템이 암호 알고리즘을 이용한다고 해서 다른 시스템에 비해 크게 느려진다고 할 수 없다.

표 1 RSA 알고리즘을 수행한 시간

	메시지 암호화	메시지 복호화	메시지 전자서명	전자서명 인증	사용권 획득 시간
512 bits	53	192	189	46	305

(키의 길이 : 64 bits 단위 : ms)

5. 결론 및 향후 과제

제안한 시스템은 공개키 암호 방식을 이용하여 사용권을 전송한다. 사용자 시스템의 사용권 관리 소프트웨어는 이 암호화된 사용권을 이용하여 소프트웨어 설치와 실행을 감시하므로 불법 복제 및 유통을 방지할 수 있다.

그러나 사용권의 파일 크기가 증가하거나, 사용자가 안전하다고 느낄수 있는 키의 크기가 증가하는 경우 속도는 지수승 만큼 느려진다. 따라서 이러한 trade-off를 고려한 최적화된 값을 찾아내는 연구가 필요하다.

참고문헌

[1] IBM ESD(Electronic Software Distribution) URL: http://www.spa.org/sigs/internetesdpoli.htm

[2] 임신영, 디지털 지적 재산권 보호를 위한 인증 응용 기술, EC/CALS 기술 워크샵 발표자료집, pp. 271-275, 1999

[3] ESD, "http://www.newengland-partners.com/RP_DEL5.html#_Toc409344544"

[4] Symantec, "http://www.symantec.com/region/kr/"

[5] Perlman, R., "An overview of PKI trust models", IEEE Network, Vol.13 No.6, pp.38-43, 1999

[6] Cramer, R., and Shoup, V., "Signature schemes based on the strong RSA assumption", Proceedings of the 6th ACM conference on Computer and communications security, pp.46 - 51, 1999