IE Interfaces
Vol. 13, No. 1, pp. 141-146, March 2000.

컴퓨터 프로그램 온라인 판매를 위한 유통 및 인증 기술

임신영[1] · 이성민[2] · 김태윤[2]

[1]한국전자통신연구원, 컴퓨터 · 소프트웨어기술연구소 / [2]고려대학교 컴퓨터 학과

An Authentication Technology for On-line Computer Program Distribution

Shin-Young Lim[1] · Sung-Min Lee[2] · Tai-Yun Kim[2]

Through an on-line software distribution, a user can get the software easily using Internet. As purchase, receipt and installation of software are executed via on-line batch process the time for software purchase and installation can be reduced. In this paper, we describe technologies for on-line software distribution and propose a secure software distribution and installation protocol for electronic commerce.

1. 서 론

오늘날 정보 통신 기술의 급격한 발전으로 인하여 인터넷을 이용한 전자 상거래가 활성화되고 있다. 초고속 정보 통신망이 구축된 환경에서 인터넷을 이용한 전자 상거래시 디지털 상품의 법적인 보호 장치와 구매자 및 판매자에게 디지털 상품의 정품 및 불법복제 확인에 대한 기술 솔루션의 제공은 매우 시급하며 중요한 부분이다. 현재 국내의 불법복제 만연 현상은 소프트웨어를 하나의 상품으로 인식하고 정당한 가격을 지불하는 사용자의 정품사용 인식결여와 이를 보증해 줄 수 있는 제도적 장치 및 기술이 부족한 것이 원인이라 할 수 있다.

전자 상거래를 통해서 온라인으로 소프트웨어를 유통시키면 시간이나 비용면에서 판매자나 구매자 모두 큰 효과를 얻을 수 있다. 하지만 소프트웨어를 온라인으로 판매했을 경우 소프트웨어가 무한대의 인가되지 않은 사용자들에게 무단으로 복제될 수 있는 문제를 갖는다. 온라인 디지털 상품 거래에 있어서, 구매자는 정가로 정품을 구입하는 동시에 자신이 구입한 상품이 정품인 것을 인증 받아야 하고, 판매자는 정품을 정가로 판매하는 동시에 본 거래에서 구매자에게 판매한 상품이 정품인 것을 인증 받아야 한다. 또한 디지털 상품을 생산한 지적 재산권자는 정품거래를 통하여 소유권에 관한 정당한 권리를 얻을 수 있어야 한다.

본 논문에서는 이러한 문제를 해결하여 상거래 주체간 신뢰성을 보장하여 온라인으로 소프트웨어를 유통시키고 불법 복제를 방지할 수 있는 모델을 제안한다. 제안한 모델은 1974년 Diffie와 Hellman (W. Diffie and M. Hellman, 1976)에 의해서 제안된 공개키 기반 암호화 알고리즘을 이용한 전자 서명을 통하여 온라인으로 정품 소프트웨어를 구매한 사용자를 인증할 수 있다. 또한 사용자의 컴퓨터 상에 상주하는 인증 서버를 통해서 프로그램 사용시 사용자의 사용권을 검사한다. 따라서 설치 후 불법 복제하여 소프트웨어를 사용하는 것을 방지할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 온라인 소프트웨어 유통기술을 기술하고 3장에서는 제안한 온라인 유통 및 정품 인증 모델을 제시한다. 4장에서는 제안한 모델과 기존의 모델을 비교 및 분석한다. 마지막으로 5장에서 결론과 향후 과제를 제시한다.

2. 온라인 소프트웨어 유통기술 소개

2.1 국내 기술

온라인으로 소프트웨어를 유통시키는 국내 기술로는 마스시스템의 S.O.Shop (S.O.Shop & SDLC, URL)이 있다. S.O.Shop은 동적 사용권 관리 시스템(DSLC : Dynamic Software License Control System) (S.O.Shop & SDLC, URL)을 이용하여 제품의 사용권

(License)을 제품으로부터 분리시킨 후 사용권만을 관리한다. 따라서 소프트웨어를 마음대로 다운받을 수는 있지만 사용권 없이는 프로그램을 실행할 수 없다. 사용권 검사는 PC상에 상주하는 사용권 관리 프로그램이 담당한다.

만약 사용권 관리 프로그램이 사용권이 없다고 통보하면 해당 제품은 작동을 중지하고 사용권이 있으면 작동을 계속한다. 따라서 정품 소프트웨어를 구입한 사용자만이 제품을 사용할 수 있다.

사용권 파일은 S.O.Shop의 비밀키로 전자 서명되어 있고 사용자의 공개키로 암호화되어 있어 사용자 이외의 사람은 사용이 불가능하게 한다. DSLC의 경우 제품 프로그램 자체는 사용권이 포함되지 않아 복사 및 확산을 오히려 권장할 뿐만 아니라 네트워을 통한 전송이 자유로워 ESD(Electronic Software Distribution) (ESD, URL)가 가능하게 되었다. S.O.Shop 사용을 위한 회원 등록시 개인 정보를 입력하면 S.O.Shop 서버로부터 회원 등록 번호를 받으며 클라이언트에서 키 생성을 하여 서버에 사용자의 공개키를 등록하면 서버로부터 서버의 비밀키로 전자 서명하고 서버가 받은 사용자의 공개키로 암호화한 사용자의 신분증 파일을 다운로드 한다.

S.O.Shop을 통한 온라인 소프트웨어 유통은 전용 클라이언트를 필요로 한다.

2.2 해외 기술

온라인 상에서 정품 소프트웨어를 다운받아서 설치할 수 있는 해외 기술로는 시멘텍(SYMANTEC) (Symantec , URL)사에서는 다음과 같은 방법을 이용한다. 시멘텍사에서 제공하는 소프트웨어는 사용자가 원하면 즉시 다운로드할 수 있다. 하지만 허가된 사용자가 아니고서는 소프트웨어를 설치할 수 없다. 따라서 정품 소프트웨어의 사용을 위해서는 지불과 등록을 통한 소프트웨어 사용권을 전달받아야 한다. 사용자가 일단 웹상에서 주문폼에 등록하고 상품에 대한 지불을 마치면 다운로드한 소프트웨어의 설치시 락(lock)을 풀 수 있는 사용권을 전자 메일을 통해서 등록한 사용자에게 제공한다. 시멘텍에서는 SSL(Secure Socket Layer)을 이용하여 등록한 사용자 정보에 대하여 인크립션을 허용하므로 사용자 정보의 안전성이 보장될 수 있다.

일단 사용자는 등록과 지불을 완료하면 시멘텍사에서는 전자 메일을 통하여 사용자에게 소프트웨어를 설치할 수 있는 키인 ELC(Electronic License Certificate) (Symantec , URL)를 전송한다. 사용자는 ELC를 이용하여 구입한 소프트웨어를 설치하여 사용할 수 있다. ELC는 전자 서명을 통하여 생성되므로 전송받은 사용자가 메시지를 변형하게 되면 전자 서명이 잘못되어 설치될 수 없다. 본 논문에서 제시하는 새로운 형태의 컴퓨터 프로그램 온라인 판매를 위한 유통 및 인증 프로토콜은 위의 S.O.Shop 및 시멘텍에서 가지고 있는 문제점을 개선한 형태로 제시되었다.

3. 온라인 유통 및 정품 인증 모델

3.1 전자 상거래 주체간 요구 사항

전자 상거래를 통해서 온라인으로 소프트웨어를 구매하기 위해서는 구매자와 유통 서버, 지적 재산권자와 유통 서버 사이의 요구 사항이 충족되어야 한다. 구매자는 자신이 구입하는 소프트웨어가 정품인지 확인할 수 있어야 한다. 또한 디지털 상품 쇼핑 및 설치가 용이해야 한다. 구매 및 사용자 정보 등록시 정보가 보호되어야 하고, 추후에 정품 구매자임을 인증하는 전자 인증서를 통해 업그레이드 및 애프터서비스를 받을 수 있어야 한다.

지적 재산권자는 자신이 유통서버에 등록한 상품의 판매 정보를 얻을 수 있어야 한다. 판매된 상품에 대해서 구매자와 피드백이 가능해야 하고 불법 사용자에 대한 판매자와 구매자간의 책임 규명이 가능해야 한다.

유통 서버는 등록된 개인 정보와 신용 정보의 누출이 없어야 한다. 또한 추후 A/S를 위한 반품 정보 처리 및 관리 기능이 있어야 하며 현재까지의 판매 상황에 대한 통계 기능이 필요하다.

이러한 상거래 주체간 요구 사항의 핵심은 누가 정품을 구매했는지를 인증하는 것이다. 정품 구매자에 대한 인증은 전자 서명 기반 전자 라이센스 기술을 이용하여 제공될 수 있다.

3.2 제안한 정품 인증 유통 모델

소프트웨어 라이센스는 크게 CPU 라이센스, 사용자 라이센스, 사이트 라이센스, 서버 라이센스로 나눌 수 있다(License type, URL; KeyServer, URL). CPU 라이센스는 사용권이 특정한 컴퓨터에만 사용권이 주어진다. 따라서 소프트웨어의 사용은 허가된 컴퓨터에서만 가능하다. 사용자 라이센스는 사용권이 특정한 사람에게 주어진다. 따라서 소프트웨어의 사용은 허가된 사용자만이 가능하다. 사이트 라이센스는 사용권이 특정한 지역에 주어지고 서버 라이센스는 서버에 연결된 모든 클라이언트에게 사용권이 주어진다. 본 논문에서 제안한 정품 인증 유통 모델은 사용자 라이센스와 ESD(Electronic Software Distribution) (ESD, URL)에 기반하여 인터넷을 통해서 소프트웨어를 다운로드할 수 있다. 하지만 유통 서버를 통해서 구매한 사용자만이 설치할 수 있도록 해주는 공개키 기반 메커니즘을 제공한다. <그림 1>은 소프트웨어 유통을 위한 전체적인 인증 과정이다.

지적 재산권자는 유통 서버에 자신이 개발한 소프트웨어를 등록하고 상품명, 회사명, 비밀키로 서명한 상품코드 등의 정보를 등록한다. 구매자는 상품 구입을 위해서 구매자명, E-mail 주소, 주민등록번호, 패스워드, 공개키 등의 정보를 등록한다. 이렇게 등록된 정보는 유통 서버의 데이터베이스에 저장되어 관리된다. 구매자 등록이 완료되면 RSA (R.L. Rivest, A.Shamir and L. Adleman, 1978)나 DSA (D. Naccache, D. M'Raihi, D.

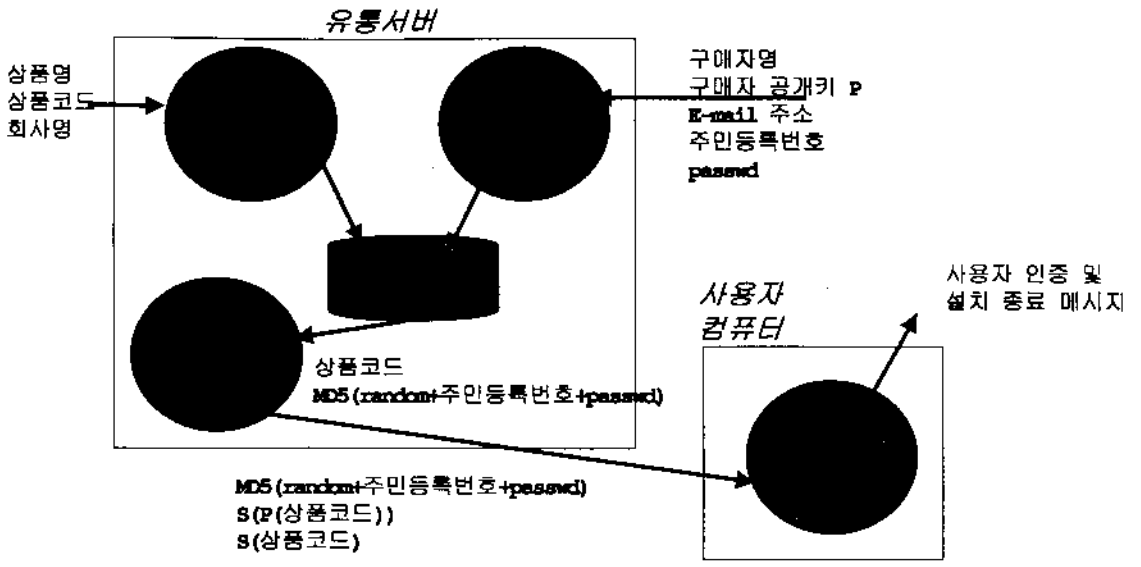

그림 1. 소프트웨어 온라인 유통 구조.

Raphaeli, and S. Vaudenay, 1994)와 같은 알고리즘을 이용하여 유통 서버의 비밀키로 전자 서명된 상품코드, 유통 서버가 생성한 난수와 사용자가 등록한 주민등록번호 및 패스워드를 MD5 (Bruce Schneier, 1996; Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, 1997)을 이용하여 생성한 해쉬 값, 마지막으로 상품코드를 사용자의 공개키로 암호화한 값에 유통 서버의 비밀키로 서명한 값을 유통 서버로부터 다운로드할 수 있다. 이 S(P(상품코드))값은 사용자가 정품을 구매한 사용자인지 불법 복제를 하여 사용하는지를 검증하고 불법 복제를 통한 소프트웨어 사용을 차단하는 데 이용된다.

사용자의 컴퓨터로 다운로드한 소프트웨어 설치 과정은 다음과 같다. 먼저 소프트웨어 설치 및 사용시 정품 구매자인지에 대한 인증을 담당하는 소프트웨어(인증 서버)를 자신의 컴퓨터에 설치한다. 이 소프트웨어는 루프백 어드레스(127.0.0.1)를 이용하여 로컬 컴퓨터상에서 인증 서버로서 작동한다. <그림 2>는 다운로드한 소프트웨어를 설치하는 과정을 나타낸다. 프로그램을 설치하기 위해서는 정해진 디렉토리에 S(P(상품코드)), S(상품코드), MD5(random+주민등록번호+passwd)와 같은 다운로드한 정보를 올려 놓아야 한다. 설치 프로그램을 시작하면 설치 프로그램은 루프백 어드레스의 미리 정해진 포트 번호를 이용하여 인증서버로 접속한다. 이때 자신의 상품코드 번호를 전송하면 인증서버는 유통 서버의 비밀키로 서명된 상품코드를 복호화하여 설치 프로그램으로 받은 상품코드와 일치하는지 비교한다. 그리고 설치 프로그램의 인스톨쉴드에서 사용자의 주민등록번호와 패스워드를 실시간으로 입력하여 인증서버가 가지고 있는 메시지 다이제스트 값과 비교한다. 현재까지의 확인 절차만으로도 정품을 구매했다는 것을 인증 가능하지만 만약 구매자가 자신의 패스워드와 비밀번호

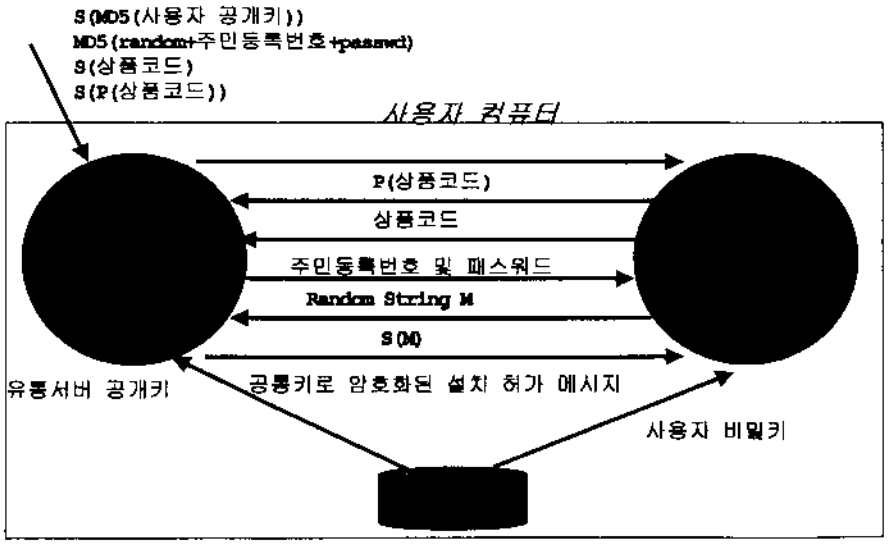

그림 2. 다운로드한 소프트웨어 설치 과정.

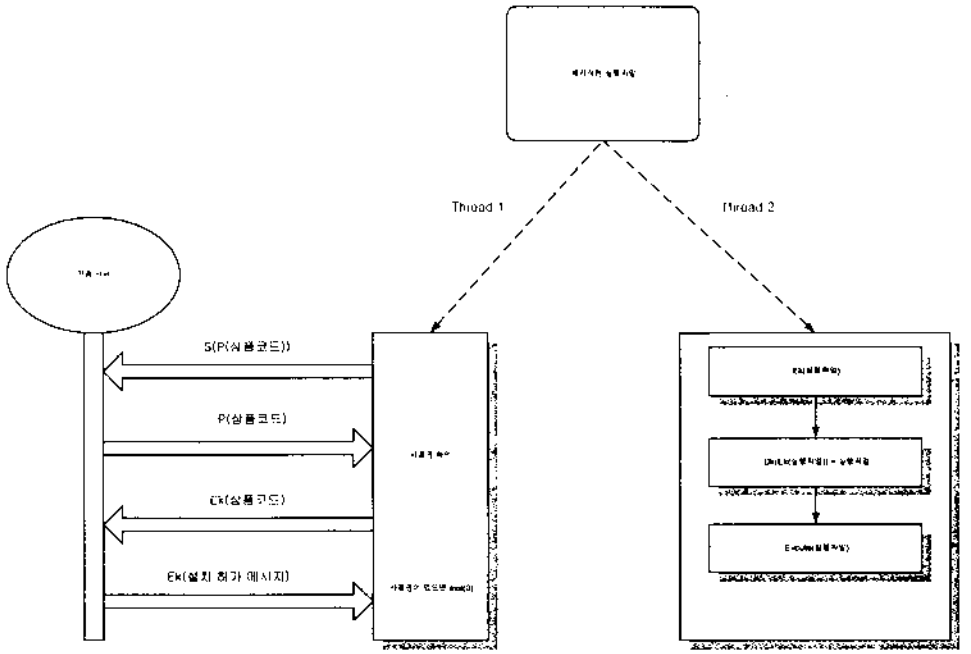

그림 3. 프로그램 실행시 불법 복제 방지 과정.

를 타인에게 공개한다면 정품을 구매하지 않은 사용자도 소프트웨어의 설치가 가능할 수 있다. 이러한 문제의 해결을 위해서 사용자의 비밀키를 이용하여 인증하는 절차를 추가하였다. 사용자의 비밀키는 신용카드 번호와 비밀번호와 같은 기능을 하는데, 이것을 타인에게 제공하는 것은 정상적인 상황에서는 발생 불가능하다고 볼 수 있다. 따라서 인증서버는 난수를 생성하여 설치 프로그램으로 전송하고 설치 프로그램은 자신의 비밀키를 이용하여 난수에 서명한 후 다시 인증서버로 전송한다. 그러면 인증서버는 사용자의 공개키를 이용하여 서명을 해독하고 그 내용이 자신이 생성한 난수와 같은지의 비교를 통해서 인증할 수 있다. 만약 비교한 결과가 같다면 설치 프로그램에게 설치를 명령하고 그렇지 않다면 설치를 종료시키는 메시지를 전송한다. 이러한 인증서버와 설치 프로그램의 상호작용은 평균 수행 시간이 약 2~3초 소용되기 때문에 시스템 전체 성능에 부하를 거의 주지 않을 정도로 충분히 경량화된 프로그램으로 구현되었다.

3.3 소프트웨어 불법 복제 방지 기술

불법적인 복제란 허가된 라이센스 개수 이상이 컴퓨터에서 작동되는 경우 이러한 프로그램을 불법적인 복제라고 한다 (KeyServer, URL). 3.2절에서와 같은 방법으로 소프트웨어 설치를 하게 되면 정품을 구매한 사용자만이 자신의 컴퓨터에 프로그램을 인스톨할 수 있다. 하지만 설치 완료 후 설치된 프로그램 파일을 다른 사용자에게 복사하여 준다면 정품 소프트웨어를 구입하지 않고도 불법적으로 복제하여 사용할 수 있는 문제가 발생한다.

이러한 문제의 해결을 위해서 본 논문에서는 소프트웨어의 실행 파일을 패키징하고 프로그램을 실행할 때마다 인증 서버로부터 라이센스에 대한 인증을 받도록 하여 불법 복제를 방지한다. 이러한 구조는 <그림 3>과 같다. 프로그램을 실행하게되면 2개의 쓰레드가 생성되어 작동한다. 하나의 쓰레드는 암호화된 실행 파일을 복호화하여 실행한다. 그리고 다른 하나의 쓰레드에서는 인증서버와의 통신을 통해서 사용권과 비밀키가 있는지를 확인한다. 이때 만약 사용권이 없다면 실행중인 쓰레드를 종료시켜 소프트웨어를 불법 복제하여 사용하는 문제를 해결할 수 있다. 만약 프로그램 실행전에 사용권과 비밀키를 통해서 정품 소프트웨어 구매자인지를 확인한다면 공개키 기반 알고리즘을 사용하므로 프로그램 실행하기까지 많은 시간이 소요되기 때문에 제안한 시스템은 인증과 프로그램 실행을 쓰레드를 이용하여 동시에 수행한다. 따라서 사용자는 사용권에 대한 인증을 하는지 모르게 투명하게 프로그램을 실행할 수 있다.

4. 온라인 유통 모델 비교 분석

본 장에서는 제안한 모델과 기존의 모델인 S.O.Shop 소프트웨어 및 Semantec사의 유통 모델을 비교 분석한다. <표 1>은 몇 가지 항목에 대해서 비교한 결과를 나타낸다. 비교 항목은 소프트웨어 구입 및 다운로드를 위해서 사용하는 클라이언트의 종류, 소프트웨어 설치 후 불법 복제하여 사용 가능 여부, 안전성 제공을 위한 기반 기술의 세 가지 항목으로 기준을 정하였다.

먼저 사용되는 클라이언트 프로그램을 살펴보면, S.O.Shop은 자신들이 만든 전용 클라이언트만을 사용하여 상품 구입

표 1. 기존의 모델과의 비교

	클라이언트 (사용자 인터페이스)	불법 복제 방지 기능	안전성 기반 기술
S.O.Shop	전용 클라이언트	O	PGP
Semantec	웹브라우저	X	SSL, 전자 서명
제안 모델	웹브라우저	O	Java JCE, SSL

및 소프트웨어 다운로드를 할 수 있다. Semantec 소프트웨어는 웹을 기반으로 하여 상품 구입(지불) 및 다운로드를 할 수 있다. 전용 클라이언트를 사용하는 것은 사용자가 반드시 클라이언트 프로그램을 설치하여야만 한다. 따라서 제안한 모델에서는 사용자에게 친숙한 웹 브라우저를 클라이언트로 사용하여 상품 구입 및 유통을 위해서 별도의 프로그램 설치를 필요로 하지 않는다.

다운로드한 소프트웨어를 설치한 후 파일을 복사하여 불법으로 사용할 수 없도록 하는 기능이 필요하다. S.O.Shop은 사용자의 컴퓨터 내에 상주하는 사용권 관리 프로그램에 의해서 설치한 소프트웨어 사용시 전자 서명된 사용권을 검사하여 인증된 사용자만이 소프트웨어를 실행할 수 있도록 한다. Semantec사의 소프트웨어는 일단 설치 후에는 파일을 불법 복제하여 사용하는 것을 방지하는 기능을 제공하지 않는다. 제안한 모델은 프로그램 실행시 사용자의 컴퓨터에서 루프백 어드레스를 이용하여 서버로 동작하는 인증서버와 통신을 하면서 사용자의 사용권을 검사한다. 소프트웨어를 사용할 수 있는 사용자인지 아닌지에 대한 검사는 전자 서명을 확인하는 등의 공개키 기반 알고리즘을 이용하기 때문에 많은 시간이 소요된다. 따라서 이러한 인증이 끝난 후 사용권이 있다고 확인된 경우만 프로그램을 수행시키면 하나의 프로그램이 실행되기까지 사용자는 많은 시간을 기다려야 하는 문제가 발생한다. 따라서 제안한 모델에서는 다중 쓰레드를 이용하여 프로그램 수행과 사용권 인증을 동시에 수행하며, 사용권이 없다고 판단된 경우는 이미 실행중인 프로그램을 종료시켜서 불법 복제를 통한 사용을 방지할 수 있다.

각 모델의 안전성 보장을 위해서 기반하고 있는 기술을 살펴보면 다음과 같다. 비교된 세 가지 모델 모두 공개키 기반 암호 알고리즘을 이용하였고 S.O.Shop은 인증 처리를 위해 pgp 암호화 라이브러리를 이용하였다. 시멘텍사의 소프트웨어는 전자 서명을 기반으로 한 ELC를 이용하였고 웹상에서의 안전한 개인 정보 등록을 위하여 SSL을 사용하였다. 제안한 모델은 Java JCE를 사용하였고 Java Servlet과 SSL을 기반으로한 웹 환경을 제공하였다.

마지막으로 각 모델의 안전성은 다음과 같이 비교될 수 있다. 시멘텍 소프트웨어는 구매자에게 ELC를 전송한다. 이것은 사용자가 제 3자에게 복사하여 준다면 소프트웨어 설치시 재사용될 수 있다. S.O.Shop은 프로그램 실행시 사용권 파일을 검사한다. 이때 사용권 파일에 유통서버가 전자 서명하고 그것을 다시 사용자의 공개키로 암호한다. 이러한 방법의 문제는 구매자가 자신의 비밀키로 복호화한 내용을 얻은 제 3자는 구매자의 공개키를 이용하여 다시 암호화하여 사용할 수 있다는 것이다. 제안한 방법은 S(P(상품코드))와 같이 구매자의 공개키로 암호화한 사용권에 다시 서명을 하므로 안전성을 보장한다.

5. 결 론

본 논문에서는 기존의 소프트웨어 온라인 유통 모델을 분석하였고 전자 상거래시 안전하게 소프트웨어를 구입 및 설치할 수 있는 온라인 소프트웨어 유통 및 정품 구매자 인증 모델을 제안하였다. 제안한 모델은 사용자에게 친숙한 웹 브라우저를 클라이언트로 이용하여 사용자 등록, 지불 및 소프트웨어 다운로드를 수행할 수 있다. 또한 공개키 기반 암호화 알고리즘과 대칭키 기반 암호화 알고리즘을 사용하여 설치시 정품을 구입한 사용자인지 인증을 한다. 설치된 소프트웨어가 불법적으로 복사되어 사용되는 것을 방지하기 위해서 유통 서버의 비밀키로 서명된 사용권 파일을 통해서 프로그램 수행시 사용권을 검사한다. 이때 사용권이 있는지에 대한 인증과 프로그램 실행을 쓰레드를 이용하여 동시에 수행한다. 따라서, 백그라운드 인증과정을 거치는 동안 사용자는 그 과정을 알 수 없도록 투명하게 수행된다. 따라서 전자 상거래시에 상거래 주체들간의 요구 사항을 모두 만족시키며 안전한 소프트웨어를 사용할 수 있는 메커니즘을 제공한다. 향후 과제로는 구매자가 원하는 다양한 종류의 라이센스에 대한 처리를 가능하게 하도록 시스템의 기능을 확장하는 것이다.

참고문헌

임신영, 하영국, 함호상, 박상봉 (1999), 디지털 지적 재산권 보호를 위한 인증 응용 기술, *EC/CALS 기술 워크샵*, 271-275.

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone (1997), *Handbook of Applied Cryptography*, CRC Press.

Bruce Schneier (1996), *Applied Cryptography*, Second Edition, Wiley.

Diffie, W. and Hellman, M. (1976), New Directions in Cryptography, *IEEE Transactions on Information Theory*.

ESD, URL: http://www.spa.org/sigs/internetesdpoli.htm

KeyServer, URL: http://www.qualitysoft.com/keywp.htm

License type, URL: http://www.software.ibm.com/is/lum/lum/lumwhtp.htm

License Use Management Project of GUIDE International Corporation (1996), Software License Use Management.

Naccache, D., M'Raihi, D., Raphaeli, D., and Vaudenay, S. (1994), Can D.S.A be Improved? Complexity Trade-Offs with the Digital Signature Standard, *Advances in Cryptology-EUROCRYPT '93 Proceedings*, Springer-Verlag.

Rivest, R. L., Shamir, A. and Adleman, L. (1978), A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Comm. ACM*, 21(2), 120-126.

S.O.Shop & SDLC, URL: http://www.soshop.co.kr

Symantec , URL: http://rigel.symantec.com

임 신 영

1983년 건국대학교 공업화학과 학사
1985년 건국대학교 화학공학과 석사
1992년 건국대학교 전자계산학과 석사
1998년 고려대학교 컴퓨터학과 박사수료
현재: 한국전자통신연구원 전자상거래연구부 선임연구원
관심분야: 인터넷 보안, 공개키 인증기관, 전자 지불, 디지털 콘텐츠 정보보호 기술

이 성 민

1997년 한림대학교 컴퓨터공학과 학사
1999년 고려대학교 컴퓨터학과 석사
현재: 고려대학교 컴퓨터학과 박사과정 재학중
관심분야: 인터넷 보안, 공개키 인증기관, 소액 전자 지불, 암호학, 분산 시스템

김 태 윤

1981년 고려대학교 산업공학과 학사
1983년 미국 Wayne State University 전산과학 석사
1987년 미국 Auburn University 전산과학 박사
현재: 고려대학교 컴퓨터학과 교수
고려대학교 컴퓨터과학기술연구소 소장