소프트웨어 저작권 보호를 위한 전자 소프트웨어 유통 프로토콜의 설계

(Design of Electronic Software Distribution Protocol for Software Copyright Protection)

김 영 준 † 이 성 민 †† 이 윤 정 †
(Young-Jun Kim) (Sung-Min Lee) (Yoon-Jung Rhee)
박 남 섭 † 이 병 래 † 김 태 윤 †††
(Nam-Sup Park) (Byung-Rae Lee) (Tai-Yun Kim)

요 약 최근 초고속 통신망을 이용한 인터넷의 대중화와 더불어 인터넷을 기반으로 하는 전자상거래가 활발해지고 있다. 특히 인터넷을 통한 전자 소프트웨어 유통(ESD: Electronic Software Distribution)은 많은 연구의 대상이 되고 있다. 하지만 기존의 모델들은 실질적인 불법복제방지와 저작권보호에 미흡하고 익명성의 보장이 어려운 단점이 있다. 따라서 본 논문에서는 공개키 기반 구조(PKI: Public Key Infrastructure)[1,2,3]에 기초하여 실질적인 저작권보호와 익명성을 보장하는 ESD 프로토콜을 제안한다. 제안된 기법은 익명을 원하는 구매자에 대한 정보를 판매자에게 제공하지 않으면서도 불법적인 복제와 유통을 억제하고 불법 복제와 유통이 발생할 시에 추적할 수 있는 장치를 제공함으로써 저작권을 보호한다. 또한 기존의 시리얼넘버(Serial Number)입력방식과 별도로 사용권을 설치해야하는 방식을 지양함으로써 사용자에게 보다 편리한 환경을 제공한다.

Abstract In recent years, e-Commerce is very active on the Internet, especially the World Wide Web along with the popularization of Internet using high-speed networks. Especially, Electronic Software Distribution(ESD) is widely being focused as one of the popular researches. However, the existing models of ESD lack substantial illegal copy protection or copyright protection as they have the shortcomings of guaranteeing anonymity of users.

This study suggests an ESD protocol that guarantees substantial copyright protection and anonymity based on the Public Key Infrastructure(PKI). The suggested method does not give the information of a buyer who doesn' t want to reveal to a seller, and protects illegal copy and distribution as well. When it happens that illegal copies are in circulation, this method provides a device to trace back its original distributor so that it helps protect the copyright. In addition, it provides more convenient environment to the user by not using the methods of serial number input and extra installation to use.

† 학생회원 : 고려대학교 컴퓨터학과
dream@netlab.korea.ac.kr
genuine@netlab.korea.ac.kr
nspark@korea.ac.kr
brlee@netlab.korea.ac.kr
†† 비 회 원 : 동양시스템즈(주) 연구원
lsm@tysystems.com
††† 종신회원 : 고려대학교 컴퓨터학과 교수
tykim@netlab.korea.ac.kr
논문접수 : 2001년 3월 26일
심사완료 : 2001년 9월 24일

1. 서 론

전자 상거래의 일반적인 정의는 네트워크와 컴퓨터 시스템을 통한 상품의 구매와 판매라고 할 수 있다[4,5]. 상거래에 필요한 정보와 처리 절차가 컴퓨터를 통해 이루어지므로, 거래의 신속성, 정확성, 효율성을 얻을 수 있고 시·공간적 제약 없이 거래를 이룰 수 있으므로, 보다 많은 거래 대상에 접근하여 거래 성사의 가능성을 높일 수 있다. 특히 최근 전자상거래를 통한 소프트웨어

판매 규모가 괄목한 만한 성장을 이루고 있다[4,6].

ESD(Electronic Software Distribution)란 인터넷을 이용한 전자상거래시장에서 소프트웨어제품을 판매하는 것을 말한다[7]. 인터넷을 통한 소프트웨어 판매는 판매자의 입장에서는 저렴한 유통 방법에 의한 상품가격의 인하와 물류 및 유통망 비용 절감을 통한 가격 경쟁력 획득이라는 여러 가지 부가적인 이득을 가지고 있다[9]. 또한 구매자의 입장에서는 제품의 업데이트를 신속히 받을 수 있고 Try-Before-You-Buy, Pay-Per-Use 등 다양한 방법으로 구매할 수 있으며 제품의 구매시 배달과정의 사고없이 신속하게 전달받을 수 있다. 하지만, 이런 여러 가지 장점에도 불구하고 ESD에는 몇 가지 문제점이 있다. 먼저 소프트웨어는 복제가 용이하고 복사본이 원본과 동일하기 때문에 인터넷을 통한 소프트웨어의 대량 불법복제와 유통이 이루어질 수 있다. 또한 인터넷은 불완전한 개방형 네트워크이기 때문에 개인의 정보보호에 취약하다[9]. 따라서 원활한 구매와 유통을 위해서는 상거래의 중요한 특징중 하나인 익명성이 보장되어야 할 것이다.

본 논문에서는 공개키 기반 구조(PKI: Public Key Infrastructure)[1,2,3]에 기초하여 사용자의 익명성을 보장하면서도 불법복제와 유통을 방지하고 사용자에게 보다 편리한 환경을 제공하기 위한 ESD 프로토콜을 제안한다. 온라인기반의 ESD 시스템에서는 소프트웨어 설치시에 소프트웨어 패키지가 자동으로 판매자 에이전트와 상호 통신하여 설치되게 함으로써 불법복제와 유통을 방지한다. 또한, 모뎀 사용자와 같이 언제나 네트워킹이 가능하지는 않은 사용자들을 위한 오프라인기반의 ESD 시스템에서는 익명성을 보장하는 구매를 위하여 인증기관인 CA를 통해서 구매만 온라인으로 하고 로컬시스템에서 설치되도록 하며 제품에 암호화된 소프트웨어 ID를 삽입함으로써 불법복제와 유통이 발생할 시에 불법배포자를 추적할 수 있는 장치를 마련한다. 또한 기존의 시리얼넘버(Serial Number)입력방식과 별도의 사용권 설치방식을 지양함으로써 사용자에게 보다 편리한 환경을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서 현재 사용하고 있는 ESD모델들에 관하여 소개하고 문제점을 제시하며 3장에서 온라인에서의 저작권보호와 오프라인에서의 저작권과 익명성 보장을 위한 ESD 프로토콜을 제안한다. 4장에서 기존의 ESD 모델들과 제안한 프로토콜의 성능을 비교 분석하고 5장에서 결론 및 향후 연구 방향을 제시한다.

2. ESD 모델

본 장에서는 현재까지 진행되어온 ESD 모델을 소개한다. 동시에 기존의 ESD 모델들을 분석하여 보고 문제점을 지적한다. 연구 결과를 토대로 사용자에게 더 편리한 환경을 제공하면서 저작권보호에 효율적인 새로운 ESD 모델을 제안하고자 한다.

2.1 선지불(Buy-first) 모델

선지불 방법은 사용자가 선택한 상품의 대금을 지불한 후 상품을 다운로드 받는 방식이다. 선지불 방법의 경우 판매자는 소프트웨어를 암호화하고 패키지화해서 다운로드 가능한 상태로 만든다. 이렇게 패키지화한 소프트웨어를 BOB(Bag-Of-Bits)[10]라고 한다.

사용자는 상품의 가격을 지불하고 BOB를 다운로드 받는다. 판매자는 사용자가 지불을 완료하면 키를 전달한다. 사용자는 전달 받은 키를 이용하여 BOB를 복호화하고 소프트웨어를 설치한다. 그림 1은 선지불 방법을 이용한 소프트웨어 구매 과정이다.

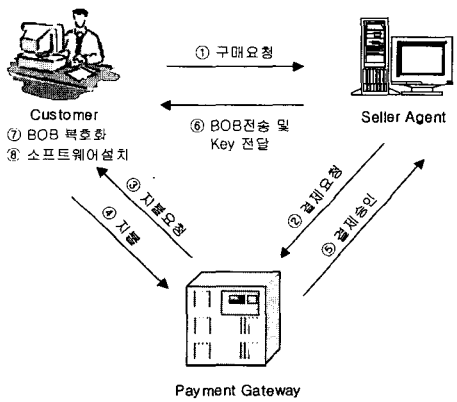

그림 1 선지불 방법을 이용한 소프트웨어 구매 과정

선지불 방법을 적용한 소프트웨어 유통 시스템은 Preview Systems사의 집락(ZipLock) 시스템을 예로 들 수 있다[11]. 집락 시스템은 대부분의 판매 시스템에서처럼 구매자의 E-mail을 통하여 키(Key)를 전달한다[12,13]. 선지불 방법은 구매 절차가 간단하지만 지불정보전송과 E-mail을 이용한 키 전송방식 때문에 익명성이 보장되지 못하고 키가 유출될 경우에 불법복제 및 유통이 가능해지기 때문에 저작권보호에 취약하다. 또한 별도의 키를 전송받아서 입력해야하는 방식으로 인해 사용자의 불편을 초래한다.

2.2 후지불(Try-before-You-buy) 방법

후지불 방법은 사용자가 소프트웨어를 제한된 환경에서 무료로 사용해 본 후 구매 여부를 결정하는 시스템이다. 판매자는 날짜에 기초하여 사용기간이나 기능에

제한을 둔 소프트웨어를 제공한다[13]. 사용자가 소프트웨어를 설치하면 제한된 기간동안 사용할 수 있다. 제한된 사용 기간이 지나게 되면 소프트웨어는 더 이상 동작하지 않는다. 사용자가 구매를 원하는 경우 온라인을 통하여 구매의사를 밝힌다. 사용자에게서 대금을 지불받으면 판매자는 키를 전송하여 사용자 시스템의 잠금(lock) 장치를 해제하도록 한다[13]. 그림 2는 후지불 방법을 이용한 소프트웨어 구매 과정이다.

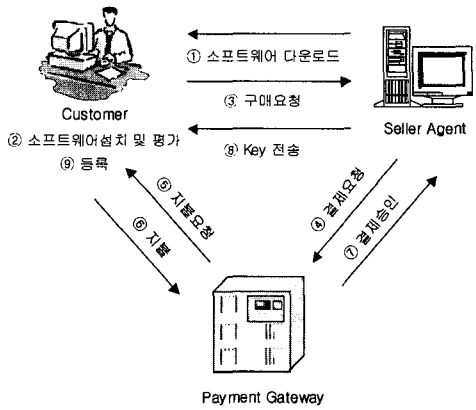

그림 2 후지불 방법을 이용한 소프트웨어 구매 과정

후지불 방법을 적용한 소프트웨어 유통 시스템은 Preview Systems사의 브이박스(Vbox) 시스템이 있다[11]. 후지불 방법을 이용한 소프트웨어 판매 방식은 선지불 방법보다 사용자의 만족이 높다. 그러나 선지불 방법과 마찬가지로 익명성이 보장되지 않고 키의 유출과 잠금 장치를 해제한 소프트웨어의 불법 복제 및 유통을 방지할 수 없다.

2.3 전자 사용권(EL: Electronic License) 모델

EL 모델은 소프트웨어의 사용권을 제품으로부터 분리시킨 후 사용권을 관리하는 시스템이다. EL 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 시스템은 소프트웨어가 실행될 때 현재 사용자가 제품의 사용권이 있는지 확인하고 확인 결과에 따라 소프트웨어가 계속 작동하던가 작동이 중지되거나 하기 때문이다. 시만텍(Symantec)사에서는 EL 모델을 적용한 소프트웨어의 온라인 판매가 이루어지고 있다[14]. 그림 3은 EL 모델을 이용한 소프트웨어 구매 과정이다.

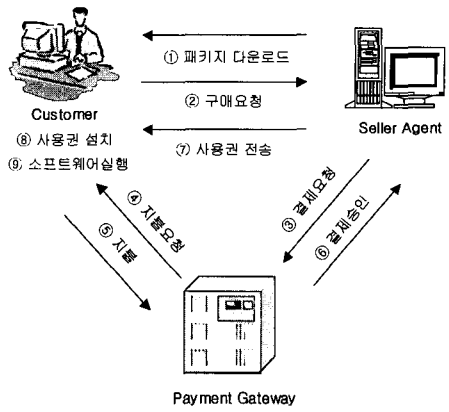

그림 3 EL 모델을 이용한 소프트웨어 구매 과정

EL 모델은 사용권을 따로 관리하므로 불법 복제 및 유통을 방지하는데 효과적이다. 그러나 익명성이 보장되지 않고 따로 사용권을 설치해야하는 사용자의 번거로움이 따르며 소프트웨어 실행시마다 사용권을 확인함으로 인한 속도저하가 발생한다.

3. 익명성과 저작권보호를 위한 ESD 프로토콜

본 논문에서 제안한 시스템은 저작권보호와 익명성보장을 위하여 온라인기반에서는 에이전트를 사용하여 시스템을 구성하였고 오프라인기반에서는 CA를 이용한 익명성이 보장되는 구매와 불법복제본의 사용자와 배포자를 확인할 수 있는 프로토콜로 구성하였다.

3.1 제안한 ESD 시스템의 구성

제안한 ESD 시스템에 참가하는 주체로는 사용자 시스템(CS: Customer System), 판매자 시스템(SS: Seller System), 판매자 에이전트(SA: Seller Agent), 인증기관(CA: Certificate Authority), 지불처리시스템(PG: Payment Gateway)이 있다. 여기서 CA는 '믿을 수 있는 제3자'(Trusted Third Party)로서 오프라인 기반의 ESD시스템에서는 전자상거래의 특징 중 하나인 익명성의 보장을 위하여 본래의 인증 기능 외에 판매자를 대신하여 금융기관에 결제요청을 하고 오프라인 기반의 ESD시스템에서 발생할지 모를 불법배포시의 불법배포자 추적을 위하여 판매자에게서 받은 거래번호(TN: Transaction Number)와 PG에게서 받은 구매자의 최소한의 정보를 관리하는 역할을 한다. 모뎀 사용자 등 불완전한 네트워크 환경에 있는 사용자들은 오프라인기반의 소프트웨어 구매를 할 수 있다. 그림 4는 제안한 ESD 시스템의 전체 그림이다.

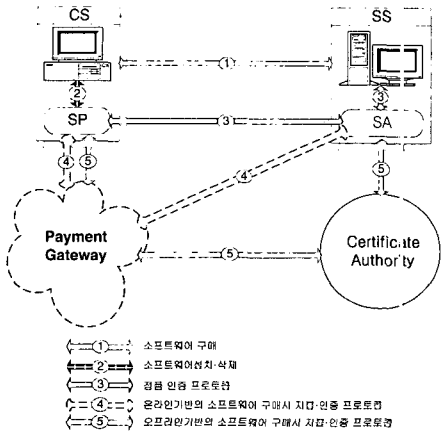

그림 4 소프트웨어 분배 및 인증 관리 에이전트 시스템

소프트웨어 구매는 CS가 SS로부터 소프트웨어 패키지(SP: Software Package)를 다운로드 받는 과정이다. 소프트웨어 설치 및 삭제는 소프트웨어를 설치하거나 다른 PC로 옮겨서 설치하기 위해 삭제할 때 CS와 SP 사이에 이루어지는 과정이다. 정품 인증 프로토콜은 소프트웨어 설치와 삭제시에 SP가 정품임을 인증하기 위하여 SP와 SA간에 이루어지는 인증 절차이다. 온라인 기반의 소프트웨어 구매시 지불·인증 프로토콜은 온라인기반의 설치를 위해 CS의 구매요청시에 SA와 PG사이에 이루어지는 승인절차이다. 오프라인기반의 소프트웨어 구매시 지불·인증 프로토콜은 오프라인기반의 설치를 위해 CS의 구매요청시에 SA와 CA, PG사이에 이루어지는 승인절차이다.

3.2 온라인(on-line)기반의 ESD 프로토콜

사용자가 소프트웨어를 구매하는 방법은 온라인 기반의 사용자들을 위한 방법과 불완전한 온라인환경(오프라인 기반)에 있는 사용자들을 위한 방법으로 나눌 수 있다. 먼저 온라인 기반의 사용자들을 위한 방법은 소프트웨어의 설치시에 사용자 시스템에 전송된 SP와 판매자 시스템의 SA사이에 자동으로 정품인증과 중복여부를 체크하므로 불법복제와 유통을 방지할 수 있다.

3.2.1 소프트웨어 구매

제안한 시스템에서 사용자가 구매요청을 할 경우에는 판매자의 홈페이지에 접속해서 원하는 소프트웨어를 선택한 후 구매요청을 한다. 판매자 시스템의 SA는 구매요청을 받게되면 PG에 결제를 요청하고 PG와 사용자간에 지불처리가 끝나면 SA에게 결제를 승인한다. 판매자는 PG에게서 결제를 승인받으면 사용자에게 SP를 전송한다. 그림 5는 온라인기반의 소프트웨어 구매과정이다.

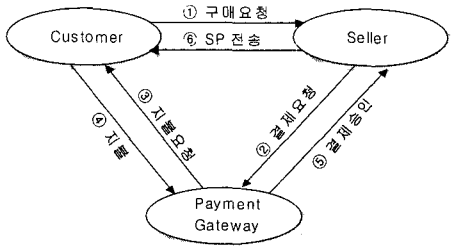

그림 5 온라인기반의 소프트웨어 구매과정

3.2.2 에이전트를 이용한 소프트웨어의 설치

본 논문에서 제안한 시스템은 기존의 사용권관리 시스템과 달리 사용자의 시스템에 별도의 사용권 관리 에이전트(LMA: License Management Agent)를 설치하지 않고 판매자 에이전트(SA)를 이용하여 정품을 인증한다.

사용자는 SS로부터 전송받은 SP의 Install 파일만 실행시키면 나머지 과정은 데몬(Daemon) 프로세스로 동작하므로 사용자는 시리얼 넘버 입력 같은 별도의 작업을 할 필요가 없다. Install이 시작되면 2개의 쓰레드가 생성되어 작동한다. 하나의 쓰레드는 암호화된 실행 파일을 복호화하여 실행하고 다른 하나의 쓰레드는 SA와 통신해서 SP가 정품임을 인증받는다. 그림 6은 SP의 패키징된 실행파일을 나타낸다.

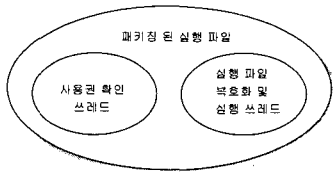

그림 6 SP 실행파일의 패키징 기법

본 시스템에서 판매자는 소프트웨어에 S_ID를 삽입할 때 제3자의 조작을 막기 위해서 S_ID를 판매자의 공개키로 암호화해서 삽입한다. 암호화된 S_ID는 오직 판매자만이 비밀키로 복호화할 수 있다.

표 1 소프트웨어 설치 절차에 사용되는 알고리즘

알고리즘	설명
P_{seller}	판매자의 공개키를 이용하여 평문을 암호문으로 암호화 한다.
S_{seller}	판매자의 비밀키를 이용하여 암호문을 평문으로 복호화 한다.
Check_dup	주어진 S_ID가 이미 등록된 것인지 확인한다.

표 2 소프트웨어 설치 절차에 사용되는 데이타 요소

데이타 요소	설명
S_ID_{SP}	SP가 가지고 있는 소프트웨어 ID
S_ID_{SS}	SS가 가지고 있는 소프트웨어 ID
RN_{SP}	SP에 전송된 등록번호
RN_{SS}	SS에 저장된 등록번호

사용자가 소프트웨어의 설치를 시작하면 SP에 포함된 사용권확인 쓰레드는 판매자의 공개키로 암호화되서 삽입된 $P_{seller}(S_ID_{SP})$를 추출한 후 SA로 전송한다. $P_{seller}(S_ID_{SP})$를 전송할 때 전송 도중 masquerade와 같은 attacker의 공격을 막기 위하여 $P_{seller}(S_ID_{SP})$에 구매자의 비밀키로 전자서명한 $S_{cust}(P_{seller}(S_ID_{SP}))$를 SP로 전송한다. SA는 SP로부터 전송받은 $S_{cust}(P_{seller}(S_ID_{SP}))$를 구매자의 공개키와 판매자의 비밀키로 복호화하여 S_ID_{SP}를 얻는다. SA는 SP가 전송한 S_ID_{SP}와 SS의 S_ID_{SS}를 비교한 후 이미 등록되어 있는 S_ID인지를 확인한다. 일련의 과정에서 중복이 없고 제대로 마치면 SA는 소프트웨어가 정품임을 확인하고 SP에게 RN(Registration Number)을 판매자의 공개키와 구매자의 공개키로 암호화한 $P_{cust}(P_{seller}(RN_{SP}))$와 OK 메시지를 전달하고 SS에 S_ID_{SS}와 RN_{SS}를 전송한다. SP는 SA로부터 $P_{cust}(P_{seller}(RN_{SP}))$와 OK 메시지를 전달받음으로써 설치를 완료하게 되고 전송받은 $P_{cust}(P_{seller}(RN_{SP}))$는 소프트웨어를 다른 PC로 옮기기 위한 삭제절차에 사용된다.

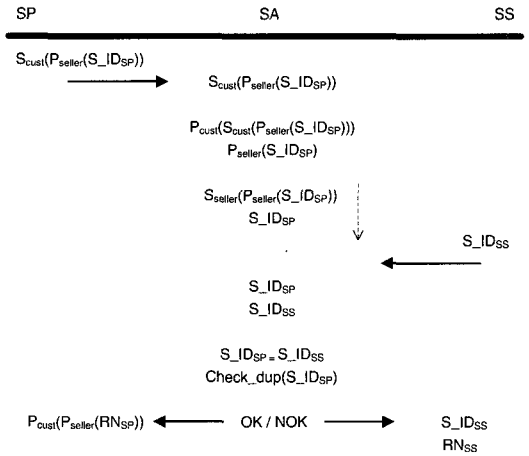

그림 7 온라인 기반의 불법복제를 방지하는 소프트웨어 설치 절차

3.2.3 소프트웨어를 다른 PC에 옮겨서 설치시

사용자가 소프트웨어 사용장소를 옮겨서 다른 PC에 설치하고 싶을 때는 기존의 소프트웨어를 Uninstall 후에 설치할 수 있다. 사용자가 Uninstall을 시작하면 SP는 소프트웨어 설치시에 SA로부터 받은 $P_{cust}(P_{seller}(RN_{SP}))$를 복호화해서 얻은 $P_{seller}(RN_{SP})$를 SA로 전송한다. $P_{seller}(RN_{SP})$를 전송할 때 구매자의 비밀키로 전자서명한 $S_{cust}(P_{seller}(RN_{SP}))$를 SA로 전송한다. $S_{cust}(P_{seller}(RN_{SP}))$를 전송 받은 SA는 구매자의 공개키와 판매자의 비밀키로 복호화하여 RN_{SP}를 얻는다. SA는 SP로부터 받은 RN_{SP}와 SS에 저장되어 있는 RN_{SS}를 비교해서 SP가 정당한 사용자임을 확인하면 SP에게 구매자의 공개키로 암호화된 OK메시지를 전달하고 SS에 S_ID_{SP}가 Uninstall 되었음을 알린다. 만약 소프트웨어를 설치한 후 갑작스런 사고로 RN_{SP}가 손상된 경우에는 최초의 $P_{cust}(P_{seller}(RN_{SP}))$에서 다시 $P_{seller}(RN_{SP})$를 복호화한다.

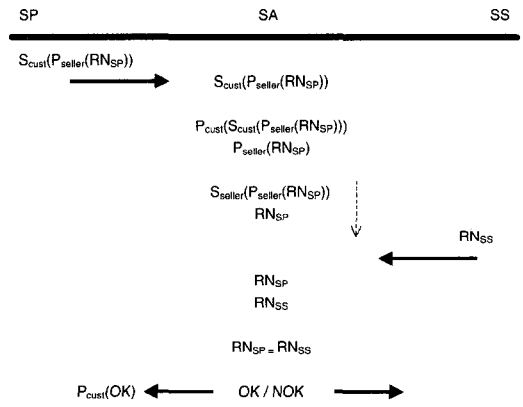

그림 8 소프트웨어 삭제 절차

3.3 오프라인(off-line)기반의 ESD 프로토콜

초고속 인터넷의 보급으로 많은 사용자들이 항상 네트워킹이 가능한 상태이지만 아직도 모뎀 등 불완전한 온라인 환경에 있는 사용자들이 많이 있다. 본 장에서는 이러한 사용자들을 위한 오프라인 기반의 저작권 보호 기법을 제시한다.

3.3.1 CA를 이용한 소프트웨어 구매

오프라인 기반의 소프트웨어 설치에서는 소프트웨어 불법배포자의 추적과 사용자의 익명성 보장을 위하여 판매자 에이전트와 CA를 이용한다. 오프라인 기반의 소프트웨어 설치를 원하는 사용자가 구매요청을 할 경우에는 판매자의 홈페이지에 guest로 접속해서 원하는 소

프트웨어와 구매방식을 선택한 후 구매요청을 한다. 판매자 시스템의 SA는 구매요청을 받게 되면 익명성이 보장되는 구매를 위하여 CA에 구매자의 인증을 요청하면서 해당거래의 거래번호(TN)를 전송한다. 이때 TN은 판매할 제품의 소프트웨어 ID(S_ID: Software ID)를 가리키는 인덱스이고 S_ID는 제품마다 유일한 번호이다. CA는 PG를 통해서 대금결제를 승인 받고, 암호화된 사용자의 정보(이름, 주민등록번호)를 넘겨받아서 TN과 함께 테이블화하여 DB로 저장한다. 저장된 정보는 추후에 불법복제로 인한 저작권분쟁이 발생할 시에 불법복제·유통된 제품에서 암호화되어 삽입된 S_ID를 추출하여 CA에 저장된 정보와 비교함으로써 불법복제와 배포자를 가릴 때 사용된다. 안전성측면에서 CA는 판매자에게서 거래번호만을 넘겨받기 때문에 사용자가 무엇을 구매했는지 알 수 없으므로 안전하다고 할 수 있다. 지불처리와 인증이 끝나면 SA는 구매자의 공개키로 SP의 실행파일을 암호화한 후 CS에 SP를 전송한다.

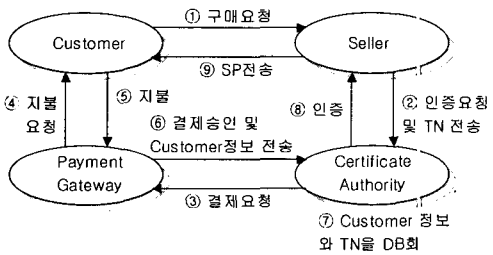

그림 9 오프라인 기반의 소프트웨어 구매과정

3.3.2 오프라인 기반의 소프트웨어 설치

모뎀환경의 사용자들은 소프트웨어의 구매만 인터넷으로 하고 설치와 사용은 오프라인 상에서 할 수 있다. 오프라인 기반에서도 마찬가지로 사용자는 Install 파일만 실행시키면 나머지 과정은 자동으로 진행되므로 별도의 프로그램 설치나 시리얼 넘버 입력 같은 과정을 거칠 필요가 없다. 일단 구매한 소프트웨어는 복제가 자유롭다.

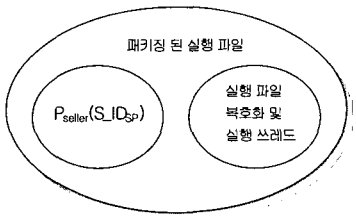

그림 10 오프라인기반의 SP 실행파일의 패키징 기법

그러나 불법 유통시에는 SP의 실행파일에 암호화되어 핑거프린팅[15,16,17,18]된 S_ID를 추적함으로써 불법배포자를 가릴 수 있고 이로 인해 불법복제를 억제하고 저작권을 보호 할 수 있다. 그림 10은 오프라인기반의 ESD에서의 SP의 패키징된 실행파일을 나타낸다.

3.3.3 불법 복제본 유통 및 배포자 확인

판매자는 $P_{seller}(S_ID_{SP})$를 삽입한 SP를 구매자에게 전송한다. SP를 구매한 사용자가 SP를 불법복제하여 사본인 SP′을 다른 사용자들에게 배포하였다면 판매자는 의심가는 SP′에서 S_ID_{SP}'을 추출하여 CA에 의뢰함으로써 SP′의 불법배포자(Traitor)[19,20]가 누구인지 밝히고 SP′의 사용자가 불법사용자(Illegal User)임을 밝힐 수 있다. 그림 11은 오프라인 기반의 저작권 보호 과정을 나타내는 그림이다.

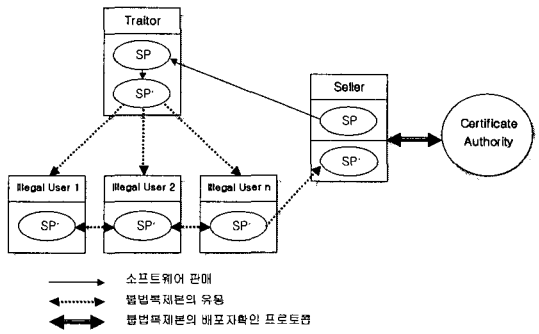

그림 11 불법 복제본 유통 및 배포자 확인 과정

3.3.4 불법복제본의 배포자 확인 프로토콜

오프라인상에서 설치 가능하게 하기 위해서는 불법복제를 막을 수는 없다. 하지만 불법으로 유통되는 복사본을 추적할 수 있는 장치를 마련함으로써 불법복제를 억제할 수는 있다.

표 3 불법복제본의 배포자 확인절차에 사용되는 데이타 요소

데이타 요소	설명
S_ID_{SP}'	SP의 복사본인 SP′이 가지고 있는 소프트웨어 ID
S_ID_{SS}	판매자 시스템에 저장되어 있는 소프트웨어 ID
TN_{SS}	판매자 시스템에 저장되어있는 해당 거래의 거래번호
TN_{CA}	CA에 전송된 해당 거래의 거래번호
C_Name	SP 구매자의 이름
C_SSN	SP 구매자의 주민등록번호

구매자가 SP의 복사본인 SP′을 불법으로 유통시키면 판매자는 의심가는 SP′에서 $P_{seller}(S_ID_{SP}')$을 추출한 후 S_{seller}로 복호화하여 S_ID_{SP}'을 얻는다. 판매자는 이 S_ID_{SP}'을 SS에 저장되어 있는 S_ID_{SS}와 비교한 후 해당되는 TN_{SS}를 CA에 전송해서 구매자확인을 의뢰한다. TN_{SS}를 전송받은 CA는 저장되어있는 TN_{CA}와 비교함으로써 구매자의 정보(C_Name, C_SSN)를 확인하고 판매자에게 전송함으로써 판매자는 불법배포자와 사용자에 대해 법적대응을 할 수 있다.

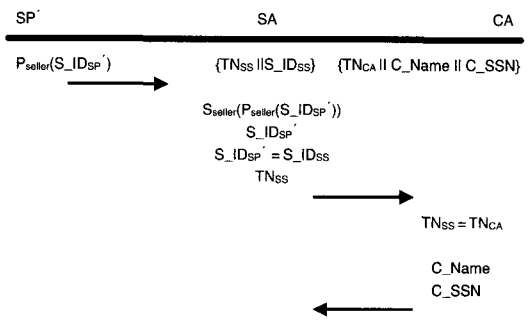

그림 12 불법 복제본의 배포자 확인 프로토콜

4. 성능 평가 및 분석

본 장에서는 제안한 ESD 프로토콜을 적용한 시스템과 기존 ESD 모델을 적용한 시스템간의 수행 모듈과 프로토콜 및 성능을 비교 분석하여 평가한다.

4.1 시스템간의 분배 및 구매 절차에 따른 수행 모듈 비교 분석

표 4는 선지불 방법의 집락(ZipLock) 시스템, 후지불 방법의 브이박스(Vbox) 시스템, EL모델의 시만텍사의 시스템 그리고 본 논문에서 제안한 시스템에서의 소프트웨어 분배 및 구매 절차에 사용되는 모듈을 비교한 것이다.

분배 절차(D)에 있어서 ESD 모델은 모두 패키지를 제작한다. ZipLock은 패키지 자체를 암호화하는 반면에 제안한 시스템은 실행파일과 소프트웨어 ID만 암호화한다. 따라서 ZipLock에서는 소프트웨어의 파일 크기가 큰 경우에 암호화하는데 오랜 시간이 소요되는 단점이 있다.

구매 절차(P)에 있어서 ZipLock은 패키지의 복호화와 잠금 해제에 시간이 소요되고 Vbox는 소프트웨어의 잠금 장치를 직접 해제해야하는 반면에 제안한 시스템은 네크워크를 통해서 자동으로 패키지와 소프트웨어의 잠금 장치를 해제한다.

관리 절차(M)에 있어서 ZipLock은 소프트웨어 판매 후 사후 관리가 필요 없다. Vbox의 경우에 제한기간이 지나면 소프트웨어를 시스템에서 삭제해야 한다. 그러나 제안된 시스템은 소프트웨어를 삭제하는 등의 추가적인 노력이 필요 없다.

4.2 제안한 시스템과 기존의 ESD시스템의 프로토콜 비교 분석

표 5는 제안한 시스템과 기존의 ESD 프로토콜을 비교 분석한 것이다. ZipLock과 Vbox는 네트워크상에 BOB나 Key가 노출되어 있기 때문에 attacker가 중간에서 intercept하여 사용할 수 있다. 하지만 제안한 시스템은 전송되는 SP의 실행파일이 구매자의 공개키로 암호화되어 있기 때문에 중간에 intercept한다 하여도 복호화하여 사용할 수 없다. ZipLock과 Vbox, EL모델은 Masquerade나 Replay Attack에 대해 취약하나 제

표 4 시스템간의 분배 및 구매 절차에 따른 수행 모듈 비교

단계	적용 모듈	집락 시스템 (ZipLock)	브이박스 시스템 (Vbox)	시만텍사의 EL을 이용한 시스템	제안한 시스템	
					On-line	Off-line
분배 절차 (D)	패키지의 제작	○	○	○	○	○
	패키지의 암호화	○	×	×	×	×
	사용권 제작	×	×	○	×	×
	사용권 암호화	×	×	○	×	×
구매 절차 (P)	패키지의 복호화	○	×	×	×	×
	패키지의 잠금 해제	○	×	○	○	○
	소프트웨어 잠금 해제	×	○	×	×	×
	사용권 복호화	×	×	○	×	×
관리 절차 (M)	소프트웨어 설치 해제	×	○	○	×	×
	사용권 관리	×	×	○	×	×

(○: Yes ×: No)

표 5 제안한 프로토콜과 기존의 ESD 프로토콜 성능 비교

비교 항목 \ 적용 시스템	집락 시스템 (ZipLock)	브이박스 시스템 (Vbox)	시만텍사의 EL을 이용한 시스템	제안한 시스템	
				On-line	Off-line
SP전송시 노출위험에 대한 대책	×	○	○	○	○
Key전송시 노출위험에 대한 대책	×	×	×	○	○
Masquerade에 대한 대책	×	×	×	○	○
Replay Attack에 대한 대책	×	×	×	○	○
소프트웨어 불법사용 방지	×	×	×	○	×
소프트웨어 불법사용자 확인기능	×	×	×	×	○
소프트웨어 불법배포자 추적기능	×	×	×	×	○

(○: High △: Low ×: None)

표 6 제안한 시스템과 기존의 ESD시스템과의 성능 비교

비교 항목 \ 적용 시스템	집락 시스템 (ZipLock)	브이박스 시스템 (Vbox)	시만텍사의 EL을 이용한 시스템	제안한 시스템	
				On-line	Off-line
익명성	×	×	×	×	○
소프트웨어 불법 복제 방지	×	×	△	○	△
소프트웨어 불법 유통 방지	×	×	○	○	○
판매자 이익보호	○	△	○	○	○
사용자 편의성	×	△	△	○	○
네트워크 비 의존도	○	○	×	△	○

(○: High △: Low ×: None)

안한 시스템은 SP에서 SA로 판매자의 공개키로 암호화되어 삽입된 $P_{seller}(S_ID_{SP})$를 전송할 때 구매자의 비밀키로 전자서명한 후 전송 도중 attacker의 공격을 막기 위해서 다시 판매자의 공개키로 암호화된 $P_{seller}(S_{cust}(P_{seller}(S_ID_{SP})))$를 전송하기 때문에 Masquerade나 Replay Attack을 방지할 수 있다. 또한 SA에서 SP로 $P_{seller}(RN_{SP})$를 전송할 때도 구매자의 공개키로 암호화한 $P_{cust}(P_{seller}(RN_{SP}))$를 전송하기 때문에 중간에 attacker가 intercept하여도 구매자의 비밀키인 S_{cust}를 모르기 때문에 복호화하여 사용할 수 없다. 제안한 시스템의 온라인 프로토콜에서는 일단 정식으로 구매한 사용자가 인증과 설치과정을 거친후에는 제 3자가 다시 설치를 할 수 없다. 제 3자가 설치를 시작하여 판매자 에이전트와의 인증과정을 거치게되면 중복이되어 설치를 거부하게 된다. 따라서 온라인상에서의 프로토콜에서는 불법사용자체가 불가능하다. ZipLock과 Vbox, EL모델은 불법사용자의 확인과 불법배포자를 추적할 수 있는 장치가 없으나 제안한 프로토콜은 의심가는 SP의 $P_{seller}(S_ID_{SP})$에서 해당 TN_{SS}와 CA에 저장되어있는 TN_{CA}를 비교함으로써 불법사용자와 배포자를 확인할 수 있다.

4.3 제안한 시스템과 기존의 ESD시스템의 성능 비교 분석

표 6은 제안한 시스템과 기존 ESD 모델의 성능을 비교 분석한 것이다. 기존의 ESD 모델들은 전자상거래에서 중요한 특징 중 하나인 익명성이 보장되지 않았으나 제안한 시스템은 사용자가 익명을 원할 경우에 CA를 통하여 익명성을 보장받을 수 있다. ZipLock과 Vbox는 키의 유출과 잠금 장치를 해제한 소프트웨어의 복제를 통해 불법복제와 유통이 가능하나 EL모델은 사용권을 관리하므로 불법 복제는 가능하나 유통과 사용은 막을 수 있다. 반면에 제안한 시스템은 소프트웨어 설치시에 SP와 SA가 상호통신하여 설치됨으로 인해 불법복제와 유통 및 사용을 방지한다. 또한 오프라인기반의 ESD 시스템에선 불법으로 유통되는 소프트웨어를 추적하고 불법 배포자와 사용자를 가림으로 소프트웨어의 저작권과 판매자의 이익을 보호할 수 있다. ZipLock과 Vbox는 시리얼넘버를 입력해야 정식으로 사용할 수 있고 EL모델도 별도의 사용권을 설치해야 하지만 제안한 시스템은 사용자가 Install만 실행시키면 시리얼넘버 입력이나 별도의 사용권을 설치할 필요없이 나머지 과정은 자

동으로 진행됨으로 사용자에게 좀 더 편리한 환경을 제공한다.

5. 결론 및 향후 연구 과제

소프트웨어 구매시에 기존의 CD-ROM 등의 매체를 이용하는 방법에서 점차 온라인상에서 ESD로 제품을 구매하는 추세가 늘어가고 있다. 이러한 시점에서 전자상거래에 필수적인 익명성과 저작권보호라는 문제를 해결하는 것은 중요하다. 본 논문에서는 PKI를 기반으로 한 익명성이 보장되는 ESD 프로토콜을 설계하였다. 온라인기반의 ESD 시스템에서는 소프트웨어 설치시에 소프트웨어 패키지가 자동으로 판매자 에이전트와 상호 통신하여 설치되게 함으로써 불법복제와 유통을 방지하였다. 오프라인 기반의 ESD 시스템에서는 CA를 이용하여 구매자의 정보가 보호되는 익명구매가 가능하게 하였고 오프라인상에서의 불법복제와 유통을 방지하기 위하여 암호화된 소프트웨어 ID를 삽입함으로써 불법복제와 유통이 발생할 시에 추적할 수 있는 장치를 마련하였다. 또한 기존의 시리얼넘버(Serial Number)입력방식과 별도의 사용권 설치방식을 지양함으로써 사용자에게 보다 편리한 환경을 제공하였다. 향후 연구과제로는 네크워크에 의존하지 않으면서 불법복제를 방지할 수 있는 연구와 오프라인상의 ESD프로토콜에서 스스로 불법복제를 감지하여 판매자에게 신고할 수 있는 장치에 대한 연구가 필요하다.

참 고 문 헌

[1] PKI, "http://www.kisa.or.kr/technology/sub1/PKI.htm"

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

[3] Oppliger, R., "Authorization Methods for E-Commerce Applications," Proceedings of the 1999 18th IEEE Symposium on Reliable Distributed Systems, pp.366-371, 1999.

[4] Kalakota, R. and Whinston, B.A., "Frontiers of Electronic Commerce," IEEE Transactions on Components Packaging & Manufacturing Technology Part C: Manufacturing, Vol.19 No.2, 1996.

[5] Yardan, S., "Evaluating the Performances of Electronic Commerce System," Proceedings of the 1997 Winter Simulation Conference, pp.1053-1056, 1997.

[6] Jutla, D., Bodorik, P., Hajnal, C., and Davis, C., "Making business sense of electronic commerce," IEEE (us), Computer, Vol.32 No.3, pp.67-75, 1999.

[7] ESD, "http://www.esd.com/"

[8] ESD, "http://www.previewsystems.com/get-started/index. html"

[9] 윤우성, 김태윤, "UML을 이용한 불법 복제 방지를 위한 ESD 서버 설계", 정보처리학회 '2000 춘계학술발표논문집, 제7권, 제1호.

[10] "http://www.esd.com/glossary/glossary1.html"

[11] Preview Systems, "http://www.previewsystems.com"

[12] ESD models, "http://www.siia.net/pubs/bookstore/items/wpe98.htm"

[13] Masud, S., "Selling bits with Electronic Software Distribution," Intertec Publishing Corporation(us), Vol.23 No.7, 1998.

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

[15] Neal R. Wagner, "Fingerprinting" IEEE Symposium on Security and Privacy, Oakland, pp.18-22, 1983.

[16] Birgit Pfitzmann, Matthias Schunter, "Asymmetric Fingerprinting" Advances in Cryptology - Euro Crypt'96, Proceedings, Springer-Verlag, pp.84-94, 1997.

[17] Birgit Pfitzmann, Michael Waidner, "Anonymous Fingerprinting" Advances in Cryptology - Euro Crypt'97, Lecture Notes in Computer Science, Springer-Verlag, Vol.1233, pp.88-102, 1997.

[18] C. Collberg and C. Thomborson, "Software Watermarking: Models and dynamic embeddings," In Principles of Programming Languages 1999, POPL'99, San Antonio, TX, January 1999.

[19] B. Chor, A. Fiat, and M. Naor, "Tracing Traitors," Advances in Cryptology-CRYPTO '94, LNCS, Springer-Verlag, pp. 257-262, 1995.

[20] Birgit Pfitzmann, "Trials of Traced Traitors," Information Hiding, Lecture Notes in Computer Science, Vol. 1174, pp.49-64, Springer-Verlag, 1996.

김 영 준

1999년 고려대학교 전산학과 학사. 2000년 ~ 현재 고려대학교 컴퓨터학과 석사과정 재학. 관심분야는 전자상거래, 네트워크 보안, 저작권보호 기법, 암호학 등

이 성 민

1997년 한림대학교 컴퓨터공학과 학사. 1999년 고려대학교 컴퓨터학과 석사. 2001년 고려대학교 컴퓨터학과 박사. 2001년 ~ 현재 동양 시스템즈(주) 주임연구원. 관심분야는 네트워크 보안, 전자상거래, 저작권보호 기법, 분산객체 시스템, J2EE 보안 등

이 윤 정
정보과학회논문지 : 정보통신
제 28 권 제 1 호 참조

박 남 섭
1998년 부산외국어대학교 컴퓨터공학과 학사. 2000년 부산외국어대학교 컴퓨터공학과 석사. 2000년 ~ 현재 고려대학교 컴퓨터학과 박사과정 재학. 관심분야는 네트워크 보안, 결함 허용 시스템, 네트워크 모니터링 등

이 병 래
1998년 고려대학교 컴퓨터학과 학사. 2000년 고려대학교 컴퓨터학과 석사. 2000년 ~ 현재 고려대학교 컴퓨터학과 박사과정 재학. 관심분야는 암호학, 네트워크 보안, 이동통신 등

김 태 윤
정보과학회논문지 : 정보통신
제 28 권 제 1 호 참조