익명성을 보장하는 ESD 프로토콜의 설계

김영준[0] 이병래 김태윤
고려대학교 컴퓨터학과
{dream, brlee, tykim}@netlab.korea.ac.kr

Design of Anonymity Guaranteed ESD Protocol

Young-Jun Kim[0] Byung-Rae Lee Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

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[1]. 하지만 기존의 모델들은 실질적인 불법복제방지와 저작권보호에 미흡하고 익명성의 보장이 어려운 단점이 있다. 따라서 본 논문에서는 익명성의 보장을 위한 ESD 프로토콜을 제안한다. 제안된 기법은 익명을 원하는 구매자에 대한 정보를 판매자에게 제공하지 않으면서도 불법적인 복제와 유통을 억제한다. 또한 기존의 시리얼넘버(Serial Number)입력방식과 별도의 사용권 설치방식을 지양함으로써 사용자에게 보다 편리한 환경을 제공한다.

1. 서론

ESD(Electronic Software Distribution)란 인터넷을 이용한 전자상거래시장에서 소프트웨어제품을 판매하는 것을 말한다. 인터넷을 통한 소프트웨어판매는 저렴한 유통 방법에 의한 상품가격의 인하와 물류 및 유통망 비용 절감을 통한 가격 경쟁력 획득이라는 여러 가지 부가적인 이득을 가지고 있다[2]. 또한 판매자의 제품은 구매자에게 배달과정의 사고없이 신속하게 전달되고 구매자는 모든 과정을 본인이 처리할 수 있다. 하지만, 이런 여러 가지 장점에도 불구하고 인터넷은 불완전한 개방형 네트워크이기 때문에 개인의 정보보호에 취약하다[2]. 또한, 전자상거래에서 안전하고 원활한 거래를 위해서는 상호신뢰가 중요하다. 따라서 본 논문에서는 사용자의 익명성을 보장하면서도 불법복제와 유통을 방지하고 사용자에게 보다 편한 환경을 제공하기 위한 ESD 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서 기존의 ESD 모델들을 분석하고 3 장에서 제안한 ESD 프로토콜을 기술한다. 4 장에서 프로토콜을 비교 분석하고 5 장에서 결론 맺는다.

2. ESD 모델

2.1 선지불(Buy-first) 모델

선지불 방법은 사용자가 선택한 상품의 대금을 지불한 후 상품을 다운로드 받는 방식이다. 선지불 방법을 적용한 소프트웨어 유통 시스템은 포틀랜드 소프트웨어(Portland Software)사의 집락(ZipLock) 시스템을 예로 들 수 있다[3]. 선지불 방법은 구매 절차가 간단하지만 지불정보전송과 E-mail 을 이용한 키 전송방식 때문에 익명성이 보장되지 못하고 키가 유출될 경우에 불법복제 및 유통이 가능해지기 때문에 저작권보호에 취약하다.

2.2 후지불(Try-before-You-buy) 모델

후지불 방법은 사용자가 소프트웨어를 제한된 환경에서 무료로 사용해 본 후 구매 여부를 결정하는 시스템이다. 후지불 방법을 적용한 소프트웨어 유통 시스템은 포틀랜드 소프트웨어사의 브이박스(Vbox) 시스템이 있다[3]. 후지불 방법을 이용한 소프트웨어 판매 방식은 선지불 방법보다 사용자의 만족이 높다. 그러나 선지불 방법과 마찬가지로 익명성이 보장되지 않고 잠금장치를 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 모델

에서 사용자는 원하는 소프트웨어를 즉시 다운로드 할 수 있다. 하지만 어떤 소프트웨어 제품이 PC 상에 설치되어 있더라도 사용권이 없으면 수행되지 않기 때문에 소프트웨어의 사용을 위해서는 지불과 등록을 통하여 사용권을 전달 받아야 한다[4]. 시만텍사(Symantec)에서는 EL 모델을 적용한 소프트웨어의 온라인 판매가 이루어지고 있다[5]. EL 모델은 사용권을 따로 관리하므로 불법 복제 및 유통을 방지하는데 효과적이다. 그러나 따로 사용권을 설치해야하는 사용자의 번거로움이 따르고 소프트웨어 실행시마다 사용권을 확인함으로 인한 속도저하가 발생한다.

3. 제안한 ESD 프로토콜

본 논문에서 제안한 시스템은 사용자의 요구에 따라 일반적인 회원구매와 익명성을 보장하는 비회원구매기능을 제공하고 불법복제방지와 사용자에게 더 편리한 환경을 제공하기 위하여 에이전트를 사용한다.

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), 지불 처리 시스템(PG: Payment Gateway)이 있다. 여기서 CA 는 본래의 인증기능 외에 판매자의 요청에 따라 금융기관에 대신 결제요청을 하고 판매한 소프트웨어 정보(Software ID: S_ID)와 구매자의 정보를 관리하는 역할을 한다. 사용자가 익명성을 필요로 하지 않을 경우에는 회원으로 가입해서 회원구매를 할 수 있고 익명성을 필요로 할 경우에는 guest 로 접속해서 비회원 구매를 할 수 있다. 그림 1 은 제안한 ESD 시스템의 전체 그림이다.

3.2 소프트웨어 구매

제안한 시스템에서 사용자가 익명으로 구매를 원할 경우에는 판매자의 홈페이지에 guest 로 접속해서 원하는 소프트웨어를 선택한 후 구매요청을 한다. 판매자 시스템의 SA 는 구매요청을 받게 되면 CA 에 구매자의 인증을 요청하면서 판매할 제품의 소프트웨어 ID(S_ID)를 전송한다. CA 는 지불처리시스템(PG)을 통해서 대금결제를 승인 받고 사용자의 정보(이름, 주민등록번호)를 넘겨받아서 S_ID 와 함께 테이블화하여 DB 로 저장한다. 저장된 정보는 추후에 불법복제로 인한 저작권분쟁이 발생할 시에 불법복제· 유통된 제품에서 S_ID 를 추출하여 CA 에 저장된 정보와 비교함으로써 불법복제와 배포자를 가릴 때 사용된다. 그림 2 는 익명성을 요구하는 사용자의 소프트웨어 구매과정을 나타낸 것이다.

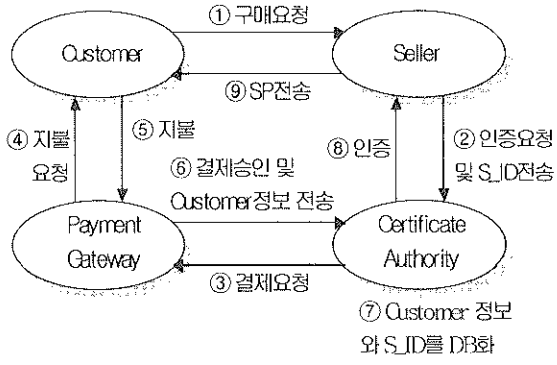

그림 2 익명성이 보장된 소프트웨어 구매과정

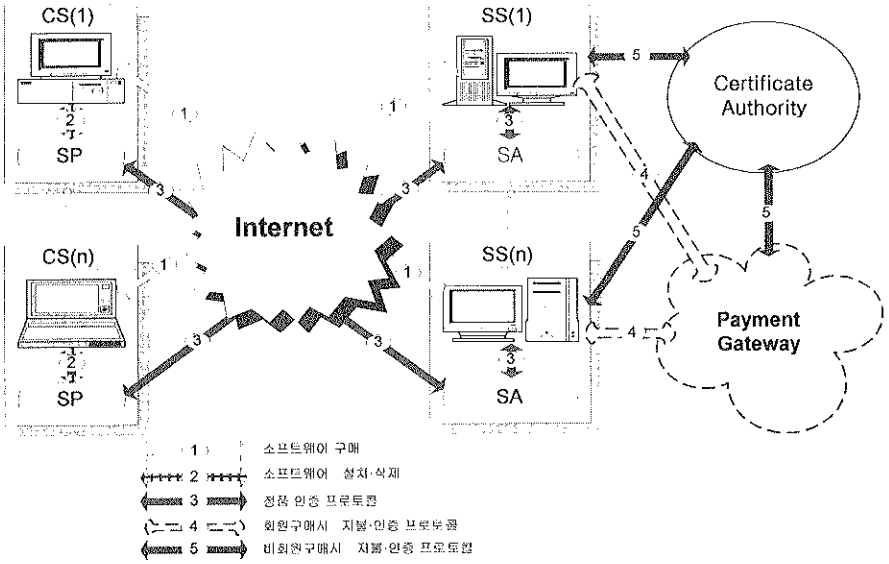

그림 1 제안한 ESD 시스템의 전체 그림

3.3 소프트웨어 설치

본 논문에서 제안한 시스템은 기존의 사용권관리 시스템과 달리 사용자의 시스템에 별도의 사용권 관리 에이전트를 설치하지 않아도 된다. 사용자는 SS 로부터 전송 받은 소프트웨어 패키지(SP)의 Install 파일만 실행시키면 나머지 과정은 데몬(Daemon) 프로세스로 동작하므로 사용자는 시리얼 넘버 입력 같은 별도의 작업을 할 필요가 없다.

표1 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.

표2 소프트웨어 설치 절차에 사용되는 데이터 요소

데이터 요소	설명
S_ID_{SP}	SP 가 가지고 있는 소프트웨어 ID
S_ID_{SS}	SS 가 가지고 있는 소프트웨어 ID
RN_{SP}	SP 에 전송된 등록번호
RN_{SS}	SS 에 저장된 등록번호

사용자가 소프트웨어의 설치를 시작하면 SP 에 포함된 사용권확인 쓰레드는 판매자의 공개키로 암호화되서 삽입된 $P_{seller}(S_ID_{SP})$를 추출한 후 SA 로 전송한다. SA 는 SP 로부터 전송받은 $P_{seller}(S_ID_{SP})$를 S_{seller}로 복호화하여 S_ID_{SP} 를 얻는다. SA 는 SP 가 전송한 S_ID_{SP} 와 SS 의 S_ID_{SS} 를 비교한 후 이미 등록되어있는 S_ID 인지를 확인한다. 일련의 과정에서 중복이 없고 제대로 마치면 SA 는 소프트웨어가 정품임을 확인하고 SP 에게 OK 메시지와 RN(Registerd Number)을 전달하고 잘못되는 경우에는 NOK 메시지를 전달한다.

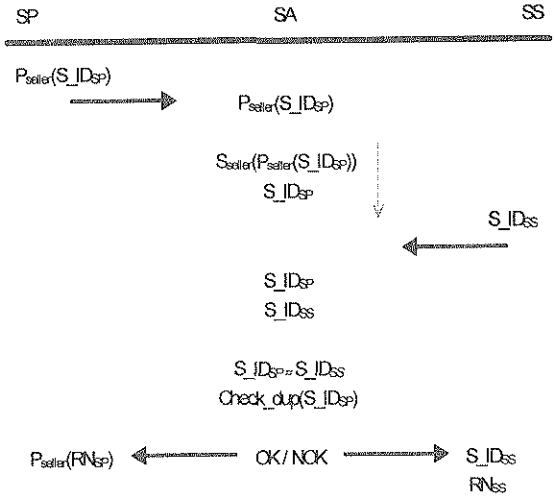

그림 3 소프트웨어 설치 절차

4. 제안한 프로토콜의 성능비교

표 3 은 선지불 방법을 이용하는 집락(ZipLock) 시스템, 후지불 방법을 이용하는 브이박스(Vbox) 시스템, EL 모델을 이용한 시만텍사의 시스템 그리고 본 논문에서 제안한 시스템의 성능을 비교 분석한 것이다.

표3 제안한 프로토콜과 다른 ESD 모델과의 성능 비교

항목 \ 시스템	집락 (ZipLock)	브이박스 (Vbox)	시만텍사 (Sym)	제안한 시스템
익명성 보장	None	None	None	High
불법복제방지	None	None	ρ	High
불법유통방지	None	None	High	High
사용자편의성	None	ρ	ρ	High
판매자이익보호	High	ρ	High	High
네트워크의존도	ρ	ρ	ρ	High

(High: High ρ: Low None: None)

5. 결론 및 향후 연구과제

기존의 ESD 모델은 불법복제방지와 저작권보호에 비중하고 익명성의 보장이 어려운 단점이 있었다. 본 논문에서는 PKI[6]를 기반으로 한 익명성이 보장되는 ESD 프로토콜을 제안하였다. 사용자가 익명으로 구매를 원할시에는 CA 를 이용하여 구매자의 정보가 보호되는 익명구매가 가능하게 하였고 소프트웨어 설치시에 SP 가 자동으로 SA 와 상호 통신함으로써 불법복제와 유통을 방지하였다. 또한 기존의 시리얼넘버(Serial Number)입력방식과 별도의 사용권 설치방식을 지양함으로써 사용자에게 보다 편리한 환경을 제공하였다. 향후 연구과제로는 모뎀사용자 등 불완전한 온라인환경에 있는 사용자들의 익명성이 보장되는 구매와 저작권보호를 위한 연구가 필요하다.

6. 참고 문헌

[1] " http://www.esd.com/esd101/index.html"
[2] 윤우성, 김태윤, "UML을 이용한 불법 복제 방지를 위한 ESD 서버 설계", 정보처리학회 '2000 춘계학술발표논문집, v.7, n.1
[3] Portland Software, "http://www.portsoft.com"
[4] 이성민, 임신영, 김태윤, "전자 상거래를 위한 온라인 소프트웨어 분배 및 정품 인증 프로토콜의 설계", 정보처리학회 '1999. 10
[5] Symantec, " http://www.symantec.com/region/kr
[6] PKI, " http://www.kisa.or.kr/technology/sub1/PKI.htm"