Client·Sever방식을 활용한 Software License 사용자 인증 통합관리시스템 개발에 관한 연구

*숭실대학교 컴퓨터학부 김재현, 주이례, 김형준, 김예은
**한국IT전문학교 정보보안학부 김진묵, 이동섭 ***부산대학교 IT응용공학과 김동완
****서울디지털대학교 박경식 *****국민대학교 이다휜
******캐드서브 구대근 윤도상 *******크로키 김도연

Software license acquisition Authority authentication management system development by Client Sever method

Jae-Hyeun Kim, Ireh-Ju, Hyuhng Joon Kim, Ye-Eun Kim
*Dept of Computer Science, SoongSil University
Jin-Mook Kim, Dong-Sub Lee **Korea IT Professional school
Dong-wan Kim ***Pusan National University
Gyeong-Sik Park**** Seoul Digital University Da-Heun Lee
Dae-Geun Koo Do-Sang Yoon ******CADSERV Do-Yen Kim *******Croquis

요 약

본 라이선스 통합관리시스템은 사용자에게는 소프트웨어 라이선스의 간편한 인증 요청과 재인증 절차를 제공하고 라이선스 발급하고 인증하는 관리자는 사용자의 현황 파악이 가능하며 언제 어디서나 간편하게 라이선스를 제공하여 많은 시간을 단축하고 라이선스 관리 비용을 절감한다. 효율적인 소프트웨어 인증관리시스템의 개발로 소프트웨어 불법적인 사용을 방지하여 건전한 생태계를 조성할 수 있다.

1. 서론

FTA(자유무역협정), 부정경쟁방지법 강화로 불법사용 기업의 수출시에 제제를 받고 있으며 글로벌 밴더(Vendor)로부터 라이선스 감사(audit) 확대되고 있다. 그러나 기업 내에서 사용 중인 소프트웨어(S.W) 라이선스 정책 이해 부족으로 설치·구매에 따른 관리 어려움이 있고, 라이선스 현황 파악이 어려운 실정이다.

더욱이 사용 기관에서는 소프트웨어 관리 전담 인력 부재로 체계적인 관리 가 미흡하고, 개발 업체들은 불법복제로 인한 프로그램 매출 감소로 인하여 수요자와 공급자간의 라이선스 분쟁이 심화되는 추세에 있다.

소프트웨어 불법적인 저작권 침해로 소프트웨어 개발사들은 경영 악화 발생하고 있다. 대표적으로는 온라인 공간과 P2P에서 불법 업로드 및 다운로드 자주 발생한다. 현재 소프트웨어 저작권침해로 인한 프로그램의 불법 복제률은 38%에 달하고 있으며 연간 피해액은 1.2조에 달하는 실정이다.

소프트웨어 불법복제란 저작권자의 명백한 동의 없이 불법적으로 소프트웨어의 내용을 복사하거나 사용하는 것을 말한다. 컴퓨터의 소프트웨어를 저작권자의 허락 없이 불법으로 복제하는 행위가 대표적인 저작권 침해 사례로 꼽히며, 이와 같은 행위는 저작권자의 재산 침해는 물론 사회적으로도 소프트웨어 산업을 위축시킬 수 있으므로 그 피해가 심각하다.

대표적인 소프트웨어 저작권(License) 침해 유형으로는 소프트웨어를 허락 없이 불법으로 복제하는 행위는 저작권 침해 유형이며 불법복제는 소프트웨어 개발 의욕을 저하시키고 소프트웨어의 가격에 불법복제에 대한 손실액을 포함시키는 부정적인 결과를 초래된다.

구분	2008	2009	2010	2011	2013	2015(%)
한국	43	41	40	40	36	35
미국	20	20	20	19	18	17
일본	21	21	20	21	19	18
호주	36	35	34	33	31	20
영국	27	27	27	26	24	22
중국	80	79	78	77	74	70
세계 평균	41	40	40	40	40	39

(그림 1) 국가별 소프트웨어 불법복제률

2. 라이선스관리시스템 요구사항

실시간 웹서버 인증 방식의 편리하고 효율적인 소프트웨어 라이선스 관리 시스템이 필요하다.

(그림 2) 목표시스템 모델

소프트웨어 불법복제를 방지하는 라이선스 인증관리 시스템으로
-공개키로 실행파일에 보호레이어로 라이선스 암호화
-비밀 키를 클라우드 서버 공간에 저장하여 요청시 인증
-대시보드 형식의 직관적인 회사 내의 인증된 사용자의 단말기에 대한 라이선스 효율적으로 발급과 관리로 소프트웨어 구입 및 배포와 유지관리 비용 절감 기대 된다

본 기술은 모바일 단말기(Smart Phone)를 단말기 인증을 이용한 개인용 컴퓨터(PC)에서 구동되는 상용 프로그램(Application)의 소프트웨어의 불법 복제를 방지하기 위한 방법을 구현하였다.

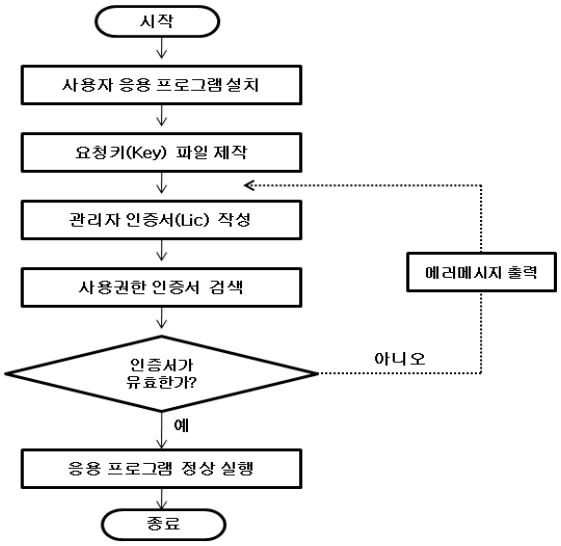
(그림 3) 시스템 개념도

본 연구는 컴퓨터 단말기의 고유정보나 휴대용단말기 저장 장치의 암호화된 고유 인증 정보를 이용하여 소프트웨어 사용자 인증 처리하는 시스템 및 방법을 개발하였다. 구체적인 방법으로는 휴대용 단말기 내부메모리에 사용자 정보를 저장하고, 상기 휴대용 단말기를 컴퓨터(P.C)용 단말기에 연결하면 소프트웨어가 구동할 때에 메모리에 저장된 권한을 부여하는 인증정보를 호출한다.

이때, 특정프로그램의 구동 시 프로그램 내에 탑재된 인증체크 부분과 스마트폰의 저장장치 혹은 메모리상의 정보를 비교하여 유효한 인증정보라고 판단되면 프로그램이 정상적으로 구동하는 방식이다.

(그림 4) 모바일인증서 비교 검증 흐름도

특정 인증관리시스템에서 인증된 사용자에게만 인증코드나 인증문자, 인증서의 다양한 인증정보를 사용자에게 전송해주고 이를 소프트웨어의 보안에 활용하는 것이다.



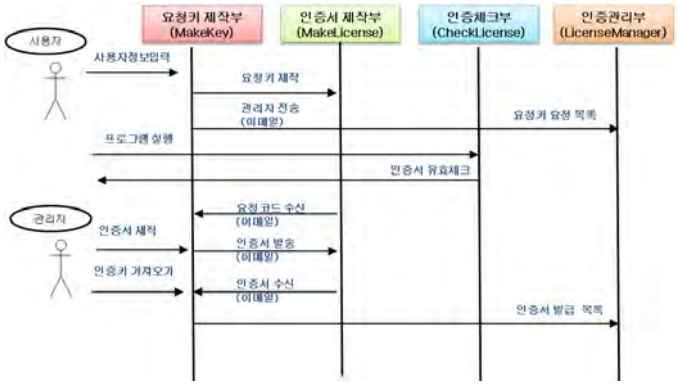
(그림 5) 복제방지 프로세스

3. 라이선스 관리 자동화 시스템 구현

윈도우 기반의 응용 프로그램이 웹상의 라이선스관리 서버에서 발급된 인증서와 동일한 정보를 포함하는 지를 판별하여 휴대용 단말기의 저장장치 상에서 실행되고 있는지를 판단하여 검증 결과에 따라 프로그램을 실행하거나 종료한다.

그림 6 에서는 사용자와 관리자 입장에서 라이선스 관리자 시스템이 프로그램을 통제하는 흐름을 도시하고 있다.

사용자 정보입력과 요청키 제작 단계를 거쳐서 관리자가 인증서 발급하여 사용자에게 전송하면 사용자는 인증저장 검토하여 정상적인 프로그램의 실행되는 일련의 과정을 자동화하였다.



(그림 6) 인증처리 흐름도

단말기로부터 제작된 요청키를 입력 정보로 사용하여 인증서를 클라우드 서버(Cloud Server)에 보관한 후에 프로그램이 구동 시에 사용자를 인증하여 사용권을 부여, 제어하는 라이선스 관리방법을 구현하였다.

라이선스의 생애주기(Lifecycle)의 관리는 회원 가입과 사용자별 인증서 프로그램에 대한 사용을 허용하는 라이선스 생성에서 폐기까지 전 과정 관리하며, 부서내의 사용자별 인증등급, 인증기간 등 등급별 관리기능 지원할 수 있다.

4. 실행파일의 복제 방지 구현 방안

윈도우 기반의 실행파일(Exe)의 암호화를 위하여 실행파일을 바이너리파일로 디컴파일한 비밀키나 개인키를 호출하는 호출메시지를 호출하는 부분을 소스코드에 삽입한 후에 다시 컴파일(Compile)하여 암호화된 레이어(Layer)를 추가하는 방식으로 실행파일이 래핑(Wrapping)을 통하여 근본적으로 프로그램의 유출을 방지한다. 또한 추가적인 보안 방법으로 사용자 컴퓨터의 시행되는 프로그램이 에이전트 방법을 이용하여 라이선스의 인증 여부로 구동되는 시스템을 구현하였다.

관리자가 데이터베이스 서버에 등록된 프로그램 목록에 해당이 되는 지를 판별하여 사용자에게 인증되지 않은 경우에는 강제적으로 해당 프로그램의 실행을 종료할 수 있다.

(그림 7) 실행파일 암호화(PKI) 복제방지방안

5. 라이선스 관리시스템 특·장점

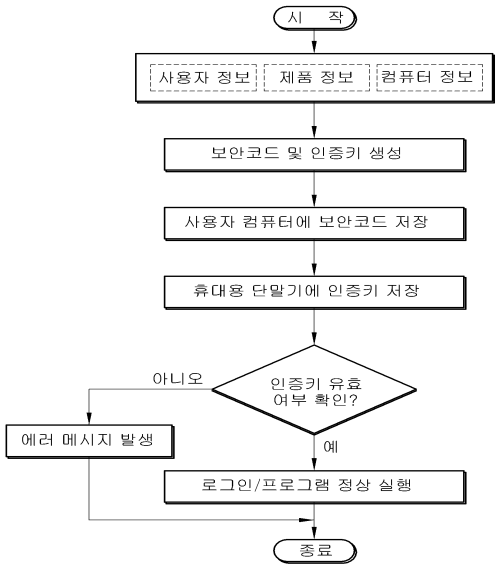
본 라이선스 관리시스템은 **기존의 시스템에 비하여 경쟁제품 대비 보안성이 우수하며, 권한 제어가 실시간 가능한 특징이 있다.** 특히 라이선스 관리자는 설정된 사용기간이나 사용가능 횟수 동안에 해당 소프트웨어를 권한을 언제 어디서나 자유롭게 중단하거나 허용할 수 있어 관리가 편리하다. 고도의 해킹이나 위·변조를 방지하기 위해서 복수의 비대칭키 사용하여 디컴파일(Decompile)이나 리버스 엔지니어링(Reverse Engineering)의 해킹과 위조 및 변조에 대응할 수 있다.

구분	기존 라이선스	신규 라이선스
인증	1 개 키 사용	2개 복수키 사용
처리	물리적 장치	프로그램 인증
보안	단일한 보안방법	Agent Wrapping 복수의 보안방법
단말기	1개 단말기 활용	복수 단말기 이용

<표1>. 기존대비 인증방식 비교표

보안코드나 인증키를 제공하고 인증키(License)를 제작하는 흐름도를 그림으로 설명하면 다음과 같다.

단말기별로 인증서를 각각 제작하여 보안을 강화하였을 뿐 아니라 사용자 스마트폰을 대표 단말기로 지정하여 한 번의 인증으로도 여러 대의 컴퓨터와 노트북의 프로그램의 사용권을 인증을 받을 수 있다.



(그림 8) 요청키 제작과 인증서 발급 처리

· **라이선스관리 효율화(Effective Managent)**
- 인증서 배포 및 인증자 및 사용자 파악 지원
- 데모, 임시, 영구 라이선스별 갱신, 폐기 관리

· **실시간 제어(Real Time)**
- 갱신, 업데이트 및 라이센스를 즉시변경 가능
- 최종사용자가 기능 요청시 즉시 적용
- 라이선스를 총체적으로 제어 관리

· **사용자중심 환경(User Centric)**
- 사용자 단말기에 라이센스 부여로 활용도가 높음
- 간편하고 안전한 라이센싱 솔루션 제공
- 단말기 장치에 상관 없이 사용자 편의를 제공

(그림 9) 스마트락 웹 화면 구현 사례

구분	USB 키락	물리장치	클라우드
보안성능	낮음	낮음	**양호함**
외장장치	필요	필요	**필요없음**
권한제어	낮음	낮음	**높음**
권한등급	어려움	어려움	**적용가능**
사용성	편리	불편	**편리**
범용성	보통	부족	**있음**
해킹위험	양호	있음	**낮음**
분실위험	있음	있음	**없음**

<표1>. 클라우드 인증방식 비교표

5. 결론

· 클라우드 서버 방식의 어플리케이션의 보안 관리

스마트락 통합 라이선스관리 시스템의 개발로 특정 실행 프로그램의 파일의 복제를 방지하여 사용 권한인증, 저작권 침해 방지를 한 번에 해결할 수 있다.

소스코드 없이 윈도우 기반의 바이너리 어플리케이션에 임의의 보안 모듈을 탑재하여 어플리케이션의 보안성을 확보하도록 하였다.

서버 기반의 라이선스 통합 관리스템을 구현하여 사용자별 인증된 프로그램 판매나자 공급자가 인증키를 배포할 때에 프로그램 마다 각각의 인증키를 배포해야 하는 노력과 관리의 비효율성을 줄일 수 있음을 확인하였다.

· 소프트웨어 현황 및 사용 통제의 시각화

라이선스의 현황을 파악 재활용하여 추가 구매 방지할 수 있어 총관리비용(TCO)가 절감되며 소프트웨어 라이선스 구매·할당의 효율화로 관리 비용 절감된다.

· 패키지 소프트웨어 개발 산업의 경쟁력 강화

라이서스 관리 시스템의 개발로 인하여 패키지형 소프트웨어 개발하는 중소 스타트업의 품질 경쟁력 제고에 도움이 될 것 있다.

소프트웨어 정품 구입 문화 확산되어 소프트웨어 개발에 대한 인식 향상된다. 이로 인하여 소프트웨어 개발사의 수익 창출이 가능해지고, 프로그램 개발자에 대한 권익 보호와 지속적인 일자리 창출 기여할 것이다.

어플리케이션의 저작권 침해를 사전에 예방하여 소프트웨어 산업 경쟁력 제고로 소프트웨어 산업 도약과 국가 차원에서 적극 육성을 위한 기반 조성된다.

소프트웨어 공정한 이용 문화의 정착으로 수요의 지속적인 창출은 고도의 창작적 소프트웨어 개발을 촉진하고, 이는 소프트웨어 산업을 비롯한 산업 전반에 긍정적인 파급효과가 기대대고 있다.

감사의 글

본 논문은 2017년 한이음 ICT멘토링 프로젝트의 결과물입니다.

참고문헌

[1] Roger S. Pressman "Software Engineering A Practltiners' Approach" 3rd Ed. McGraw Hill

[2] 휴대용 단말기를 이용한 소프트웨어 복제방지 및 권한인증 장치 및 그 방법 특허출원서, 캐드서브 구대근, 2014. 2

[3] BSA(2016. 5) 세계 소프트웨어연합(BSA | The Software Alliance)의 글로벌 SW시장규모보고서, 소프트웨어 정책연구소 자료 참, 2016. 9.