# 보안과 레지스트리 감시를 이용한 소프트웨어 설치 관리 시스템

황기태*° 주희경* 고진수* 김남윤**
* 한성대학교 컴퓨터시스템공학부
** 한성대학교 정보공학부
calafk°@hansung.ac.kr, angellll@empal.com, kkossu@empal.com,
nykim@hansung.ac.kr

# Installation and Management of the Software using Security Mechanism and Registry Monitoring

Kitae Hwang*° Hee Kyung Ju* Jin Su Ko* Nam Yun Kim**
* Division of Computer System Engineering, Hansung University
** Division of Information Engineering, Hansung University

요 약

본 논문은 불법 소프트웨어가 조직 내에 설치 사용될 수 없도록 소프트웨어를 설치하고 관리하는 시스템 모델을 제안한다. 모든 소프트웨어는 서버에서 압축 관리되며, 인증 받은 클라이언트만이 반드시 서버로부터 소프트웨어를 다운로드 받아 설치한다. 또한 주기적으로 클라이언트는 레지스트리를 검색하여 불법 소프트웨어의 설치 여부를 검사하여 서버에 보고한다. 본 논문에서 제안된 시스템은 정품 소프트웨어의 불법 사용 방지뿐만 아니라 라이센스 통제와 소프트웨어 관리의 용이성의 장점을 가진다.

## 1. 서론

우리나라 정보화 산업의 매우 빠른 발전으로 인해 소프트웨어 불법 복제에 따른 지적 재산권 침해 사례가 늘고 있으며 이는 결국 소프트웨어 개발을 저해하는 부메랑으로 돌아오게 되는 문제점을 낳게 된다[1].

현재 불법 소프트웨어의 사용을 막기 위한 많은 방법들이 개발되고 있다. 불법 복제를 막는 방법으로서 CD 복사 방지 방식[2]이나 USB 포트나 병렬 포트에 하드웨어 키 모듈을 설치하여 하드웨어 키가 없이 소프트웨어를 컴퓨터에 설치할 수 없도록 하는 방법이 있다. 또 소프트웨어의 설치를 관리함으로써 불법 소프트웨어의 사용을 막는 방법으로 주로 소프트웨어적으로 이루어진다. 이 방법은 클라이언트 컴퓨터에 특정 소프트웨어를 구동하여 설치된 소프트웨어 리스트를 관리용 컴퓨터에게 주기적으로 전송한다[3].

불법 소프트웨어의 사용을 막는 이러한 방법들은 몇 가지 문제점을 가지고 있다. 하드웨어 키를 사용하여 불법 복제를 막는 방법은 소프트웨어의 판매 단가가 올라가기 때문에 소프트웨어 제작사들이 이 방법들을 거의 채택하지 않고 있다. 클라이언트 상에 설치된 불법 소프트웨어를 서버가 단순 모니터링하여 불법 소프트웨어의 설치를 가려내는 방법 또한 CD의 불법 복사 및 유출, 분실의 가능성, 재 설치 시의 번거로움, 라이센스(license)의 카피 수에 대한 실시간 통제가 되지 않는 점 등의 문제점을 해결하지 못한다.

본 논문은 보안 체계와 레지스트리 검색으로 통해 불법 소프트웨어의 설치를 감시하는 새로운 방법을 제안한다. 클라이언트 컴퓨터는 대리(agent) 프로그램을 이용하여 서버로부터 정식 소프트웨어를 다운 받아 설치한다. 이 때 소프트웨어의 불법 유출을 막기 위해 인증, 암호화와 같은 보안 기법을 사용한다. 따라서 그룹 내에서 정품 소프트웨어의 복사본을 만들 필요가 없으므로 정품 소프트웨어의 유출 가능성이나 정품 소프트웨어의 원본 CD의 분실 가능성이 없으며, 라이센스 카피 수의 실시간 통제가 가능하다는 장점을 가진다. 클라이언트 컴퓨터상의 대리 프로그램은 불법으로 설치된 소프트웨어를 모니터링하여 서버로 통보한다.

## 2. 시스템 모델

SAP 을 구성하는 하드웨어 요소는 그림 1 과 같이 Server 컴퓨터와 Client 컴퓨터이며 인적 요소로는 조직의 구성원인 User 와 관리자 Manager, 소프트웨어 요소로 PCA(사설 인증 서버), IMS(Installation Management Server), MAP(Monitoring Agent Program)등이다. IMS 와 MAP 은 Server 와 Client 에서 항상 실행중인 상태로 설정되며 PCA 는 Client 에 인증서를 발급하고 인증서를 관리하는 소프트웨어 요소로서 Server 에서 실행된다. Server 는 조직 내의 모든 정품 소프트웨어를 압축하여 저장한다.

SAP 시스템이 동작하는 대략적인 과정은 다음과 같다. User 혹은 Manager 가 Client 를 초기 세팅할 때 Server 의 PCA 에 접속하여 인증서를 발급 받아 Client

컴퓨터 상에 저장한다. User 가 Client 에 소프트웨어를 설치하고자 하는 경우 MAP 을 이용하여 IMS 에 접속하고 인증 절차를 거친다. IMS 는 세션 키(session key)[4,5]를 생성하고 Client 의 인증성에 포함된 공개키(public key)로 이 키를 암호화하여 MAP 에게 전송한다. MAP 은 암호화된 메시지를 개인키(private key)로 복호화하여 세션 키를 확보한다. MAP 은 정품 소프트웨어 리스트를 요청하여 전송 받은 후 설치를 원하는 소프트웨어를 요청한다. IMS 는 세션 키로 소프트웨어를 암호화하여 MAP 에게 보낸다. MAP 에 세션키로 소프트웨어를 복호화하고 이를 Client 에 설치한다. 설치가 종료되는 즉시 MAP 은 세션 키로 전송 받은 데이터를 모두 삭제하여 정품 소프트웨어의 유출을 막는다

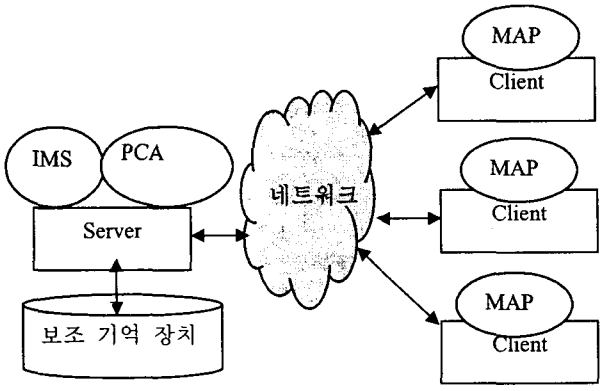


그림 1 SAP 시스템 구성

### 3. 보안 설계

SAP 시스템은 Server가 가진 정품 소프트웨어가 조직 내의 User나 외부의 염탐자에게 유출되는 것으로부터 보호하고 Client 상의 MAP과 IMS의 통신 동안 내부나 외부의 악의적인 사람들로부터 데이터 변조나 침입을 막기 위해 보안 메카니즘을 도입하였다.

조직의 구성원이 아닌 사람에 의해 SAP 시스템의 정품 소프트웨어나 기타 정보들이 유출되는 것을 막기 위해서는 세션의 시작 시점에서 MAP에 대한 인증이 필요하다. 인증(Authentication) 이란 한 객체(Entity)가 자신이 제공한 정보의 소유자가 맞는지를 신뢰할만한 인증기관(Cerificate Authority)에 의해 확인되는 과정이다. 인증을 위해서는 인증 기관(CA)으로부터 인증서가 발급되어야 한다[4,6].

### 4. 소프트웨어 설계

#### 4.1 IMS 설계

IMS 모듈의 내부 구조는 그림 2 와 같이 IMS 세션 관리자, 소프트웨어 등록 모듈, 압축 모듈, DB 관리자, 암호화/복호화 모듈, 인증 모듈, 그리고 UI 모듈로 구성된다. IMS 의 하부에는 MS-SQL Server 가 설치되어 있으며, Windows 2000 Server 의 한 부분인 인증 서버 PCA 가 위치한다. IMS 에 존재하는 데이터 저장소는 압축된 소프트웨어가 저장되는 저장소와 SAP 시스템의 관리를 위해 필요한 DB 테이블 저장소, 그리고 PCA 에서 발급된 인증서의 복사본이 저장되는 저장소의 3 부분으로 분류된다.

IMS 세션 관리자는 MAP으로부터의 네트워크 접속과 함께 설치 세션과 보고 세션의 수행을 관리하는 기능을 수행한다. 소프트웨어 등록 모듈은 새로운 소프트웨어가 도입되는 등의 이유로 하여 Client에서 설치할 소프트웨어를 Server에 등록하는 기능을 수행한다. 압축 모듈은 소프트웨어 등록 모듈에 의해 호출되는 모듈로서 도입된 소프트웨어를 압축하는 기능을 제공한다. DB 관리자는 SAP 시스템에 필요한 DB 테이블에 대한 액세스를 관리하는 모듈이다. 암호화/복호화 모듈은 각 세션에서 MAP으로 전송할 메시지를 암호화하거나 MAP으로부터 전송된 메시지를 복호화하는 기능을 제공한다. 인증 모듈은 Client의 인증을 위해 PCA에 의해 발급된 인증서 복사본이 들어 있는 시스템 저장소에서 인증서를 찾고 읽는 기능을 제공한다.

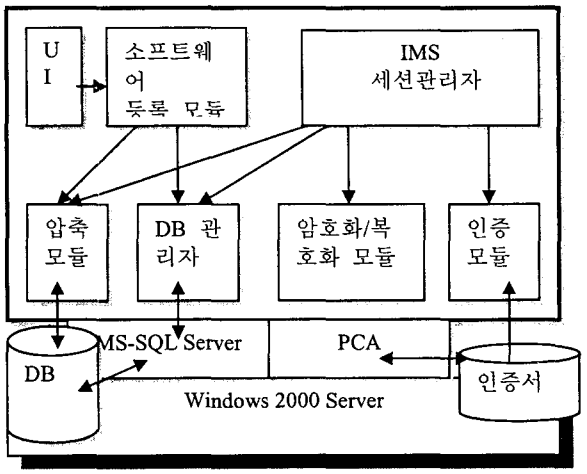


그림 2 IMS 의 구조

#### 4.2 MAP 설계

MAP은 Client에서 실행되는 SAP 모듈로서 Client 컴퓨터의 사용자인 User로부터 소프트웨어 설치 요구를 받아 IMS에 접속하여 새 소프트웨어를 Client에 설치하는 기능과 주기적으로 Client 상에 설치된 소프트웨어 리스트를 조사하고 불법으로 설치된 소프트웨어를 조사하여 IMS에 보고하는 기능을 수행한다. MAP은 그림 3 과 같이 구성된다.

Client의 인증서와 개인키는 Client의 User 혹은 Manager에 의해 Server의 PCA로부터 인증서를 발급받은 후 Client 컴퓨터의 시스템 파일 속에 기록된다. MAP은 자신이 설치한 정품 소프트웨어의 리스트를 가지고 있으며 이 리스트는 보안을 위해 디스크 상에 저장하지 않고 메모리 공간에 저장 유지한다. 이 리스트의 복사본이 Server에도 역시 저장되어 있어 MAP 프로그램이 비 정상적으로 종료하거나 리스트를 손실하였을 때 Server로부터 복구할 수 있다.

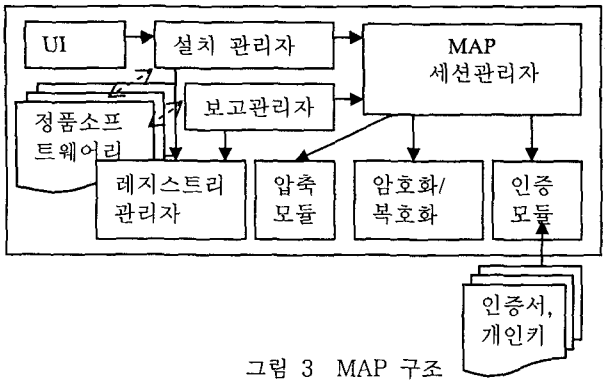


그림 3 MAP 구조

### 4.3 시스템 레지스트리(Registry) 검사

윈도우의 설치 프로그램(Install Shield)에 의해 설치된 모든 소프트웨어들은 윈도우의 시스템 레지스트리에 기록된다. 윈도우에서 실행되는 정품 소프트웨어들은 대부분 윈도우 설치 프로그램인 Install Shield 를 이용하여 설치되도록 제작되었다. MAP은 레지스트리를 검사하여 현재 설치된 소프트웨어 리스트를 확보하고 이를 자신이 설치한 정품 소프트웨어의 리스트와 비교하여 허락되지 않은 불법 소프트웨어를 판별한다.

## 5. 시스템 구현

본 장에서는 SAP 시스템의 구현에 대해 기술한다. 서버와 클라이언트간의 메시지 보안을 위해 마이크로소프트사의 CryptoAPI 를 사용하였다. 이 API 는 ASN.1 에 정의된 인코딩/디코딩, 해쉬, 인증서 관리, 암호화, 복호화 등의 기능이 포함되어 있다.

그림 4 는 서버에서 IMS 를 이용하여 새로운 소프트웨어 ALSee32 를 등록하고 있는 화면이다.

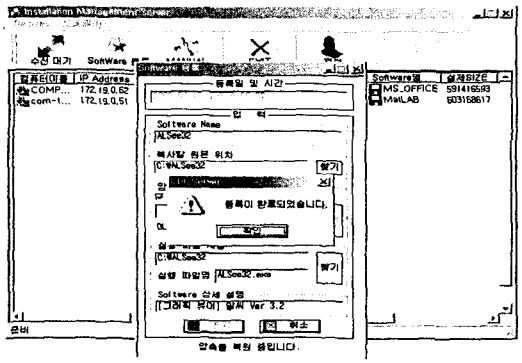

그림 4 서버에서 새로운 소프트웨어 등록 화면

그림 5 는 클라이언트에서 MAP 프로그램을 이용하여 서버에 등록된 소프트웨어를 다운 받아 자동 설치하는 과정이다. 그림 6 은 클라이언트 컴퓨터에 불법으로 설치된 *JBuilder 7.0* 과 *Visual Studio 6.0* 이 MAP 에 의해 발견되어 서버의 IMS 로 통보된 서버 화면이다.

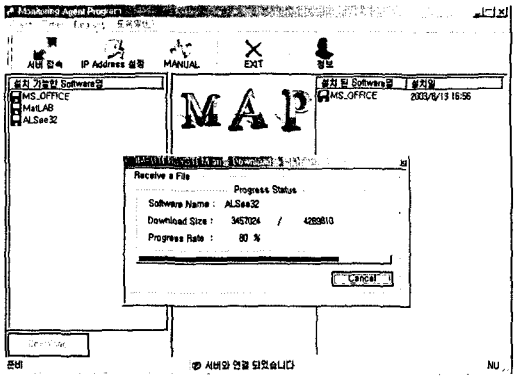


그림 5 클라이언트에서 서버로부터 소프트웨어 설치

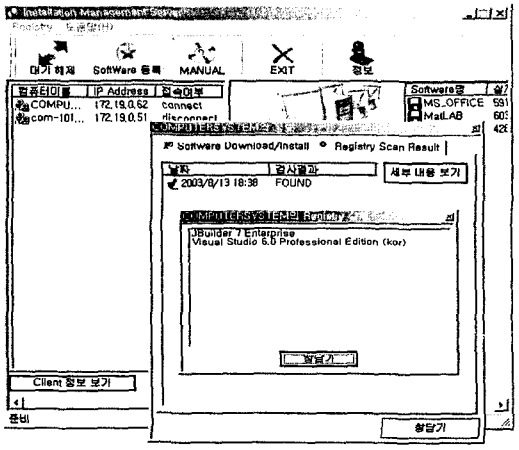


그림 6 발견된 불법소프트웨어가 서버에 보고된 화면

## 6. 결론

본 논문에서는 불법 소프트웨어의 설치 및 사용을 막기 위한 시스템 모델을 제안하였다. 모든 소프트웨어는 서버에서 관리하며 클라이언트는 오직 서버로부터 다운받아 설치하도록 한다. 불법으로 설치된 소프트웨어는 레지스트리를 검색하여 서버에 자동 통보된다.

## 참고문헌

[1] 월간 SW 저작권, SPC 집계 2002 년 S/W 불법복제 조사 리뷰, 2003 년 3 월 호.

[2] 골든 시큐리티㈜, 홈페이지: http://www.goldensecu.co.kr.

[3] 체키㈜. 홈페이지: http://www.checki.co.kr.

[4] 박창섭, *암호 이론과 보안*, 대영사, 1999.

[5] S. Burnett and S. Paine, *RSA Security' s Official Guide to CryptoGraphy*, RSA Press, 2001.

[6] R. Housley, W. Polk, W. Ford, and D. Solo, *Internet X.509* Public Key Infrastructure: Certificate and CRL Profile. RFC 2459, IETF, 1999.