한국 CAD/CAM 학회 논문집
제 11권 제 5호 2006년 10월 pp. 327-334

기술논문

설계정보 유출방지를 위한 정보보안시스템 설계 및 구현

장황배*, 이호신**

Design and Implementation of Information Security System to Prevent Leakage of Drawing Information

Chang, H. B.* and Lee, H. S.**

ABSTRACT

Recently, security incidents are growing rapidly in which internal employees let the drawing leak out to competitors or other countries. This type of security incidents has a characteristic that it occurs less frequently than other types of security incidents such as network or server security incident, but the damage is a lot more serious. The existing information security technologies to prevent internal information from being leaked out are only applicable to general documents(office documents, web pages and image files in which data are encrypted one by one). However, architectural drawings made up of collection of files with various formats(extensions) have problems with the process speed of en(de) cryption and accuracy, so the developments of security technologies by new methods are required. In this study, we design and develop a security technology based on work area with which users can protect the leakage of critical information in the kernel level while maintaining their work environment when they have to use sharing information that cannot be managed by the unit of file. As a result, we developed the "Virtual Secure Disk" which allows only authorized users and applications to have an access to drawings, and have verified its security by applying it to the actual company.

Key words : CAD Security, Virtual Secure Disk, Application Access Control, Application Programming Interface Hooking, System Service Table Hooking

1. 서 론

정보기술의 발달로 인하여 정보에 대한 획득 및 유통이 용이해짐에 따라 원활하고 효율적인 업무환경이 가능하여졌으나, 내부 및 외부 사용자에 의한 기업 내 중요정보의 불법적인 정보유출과 같은 역기능도 동시에 발생하고 있다.

외부 사용자의 내부 중요정보에 대한 접근제어를 위하여 가상 사설망(Virtual Private Network), 정보보안 프로토콜(Secure Socket Layer), 침입탐지 시스템(Intrusion Detection System), 침입차단 시스템(Intrusion Prevention System) 등과 같이 네트워크 및 서버에 대한 정보보안 기술이 개발되었지만 내부 사용자에 의한 정보유출을 방지하는 기술개발은 아직 미비한 상태이다.

내부 사용자는 업무 특성상 불가피하게 기업 내 중요정보에 접근이 가능하여야 함과 동시에 접근한 정보에 대한 유출을 방지해야 하는 양면성을 가지고 있기 때문에 업무의 효율성 및 기술적 한계성 등의 문제로 인하여 정보보안정책이나 내부사용자의 보안의식 등에만 의존하는 것이 내부정보 유출방지를 위한 최선의 대응책 일 수밖에 없는 상황이다. 따라서 내부 사용자에 의한 정보유출을 적절히 통제하면서 업무 효율성을 떨어뜨리지 않는 보안기술의 개발이 절실히 필요하다[1].

본 연구에서는 일반문서와 달리 설계도면과 같이 다양한 파일형식으로 구성된 중요정보가 내부 사용자에 의하여 부적절하게 유출되는 것을 방지할 수 있는 작업영역 기반의 중요정보 보안기술을 개발하였다[2].

*교신저자, 정회원, 소프트캠프(주) 정보보안기술연구소 책임연구원
**아이오와 주립대학교 교수
- 논문투고일: 2005. 08. 18
- 심사완료일: 2006. 04. 25

개발된 기술은 작업자의 컴퓨터시스템에 가상보안디스크(Virtual Secure Disk)를 생성하고 보안이 요구되는 설계 또는 개발 업무를 진행할 경우, 인가된 사용자 및 응용 프로그램의 모든 작업결과를 가상보안디스크 내에만 저장가능하게 하고, 인가되지 않은 사용자나 다른 응용 프로그램들은 가상보안디스크에 접근(읽기 또는 쓰기)하지 못하도록 한다.

2. 선행 연구

내부 중요정보에 대한 유출을 방지하기 위하여 보안이 요구되는 정보만을 별도로 묶어 관리하면서 이 정보에 접근을 요청하는 사용자가 인가된 사용자인지를 확인하여 접근여부를 결정짓는 기술이 개발되었다. 그러나 이 기술은 인가된 사용자 스스로가 중요정보를 유출할 경우 해결방법이 될 수 없다. 또한 최근의 업무환경은 복잡하고 전문적인 기술개발을 위하여 인가된 다수의 사용자가 업무의 효율성을 유지하면서 정보를 사용하여야 하기 때문에 사용자에 대한 번거로운 확인절차 없이도 중요정보에 대한 접근제어가 이루어질 수 있는 기술을 요구하게 되었다[1].

이에 따라 중요정보가 유출될 수 있는 경로(보안취약점)를 분석하여 이를 해결하기 위한 선행연구로서 장치제어 기술과 문서보안 기술 등이 개발되었다.

2.1 장치제어 기술

이동 저장장치(예를 들어, USB Memory, CD, Disk 등)를 통하여 중요정보가 유출될 수 있는 경로를 제어하여 정보유출을 방지하는 기술이다. 이 기술은 조직 차원에서의 정보보안 정책수립 및 적용이 어려우며, 사용자 컴퓨터 시스템에 설치된 다양한 장치들에 대하여 유출경로를 모두 통제한다는 것은 업무의 제약없이는 불가능하기 때문에 단순 작업을 수행하는 일부 내부 사용자에게만 적용할 수 있다는 문제점이 있다.

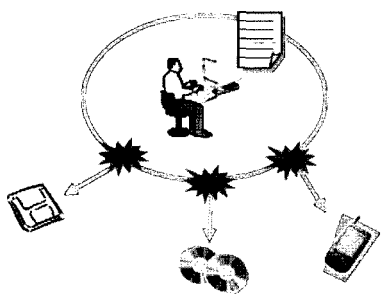


Fig. 1. 장치제어를 통한 내부정보 유출방지.

2.2 문서보안 기술

문서보안 기술은 정보를 포함하고 있는 전자문서의 생성에서부터 사용, 전달, 폐기에 이르기까지 전 구간에 대하여 정보를 보안하기 위한 기술로서 사무용 문서 작성을 위한 응용 프로그램(Notepad, Word, Excel 등)을 제어하여 사용자의 권한에 따라 전자문서의 무분별한 사용을 제한한다. 이 기술은 사용자의 업무 환경 변화를 최소화하면서 단일한 파일형식을 가지고 있는 일반 사무용 문서파일, 웹 페이지, 그림파일 등에 적용이 가능하다[2].

그러나 사무용 문서작성을 위한 응용 프로그램의 파일 입출력 과정을 프로그램마다 분석하여 적용하기 때문에 해당 응용 프로그램에 종속될 수 밖에 없으며, 응용 프로그램과 파일형식(확장자)을 연결(1:1)하여 암호화하고 이를 제어함으로써(MS Word : DOC, MS Excel : XLS) 다른 파일형식으로의 변환이 불가능하다. 또한 응용 프로그램의 고유기능 중 일부분을 사용하지 못하는 경우가 많이 발생하기 때문에 업무의 효율성이 많이 떨어지고 응용 프로그램이 개선 될 때(upgrade)마다 새로운 파일 입출력에 대한 새로운 분석이 필요하다.

2.3. 공유파일 형식 개발

윈도우즈 기반의 도면 설계프로그램으로 작성된 파일을 보호하기 선행연구로서 제3의 사용자가 설계도면 파일을 편집하거나 출력하는 작업을 제한하는 'Intermediate Data Format(DWF, PDF 등)'에 관한 연구도 진행되었다. 'DWF(Design Web Format)'는 작업을 함께 진행하는 개발자들이 설계도면 정보와 의미를 교환하기 위하여 개발되었으며, 파일 내에 정보를 편집할 수 없도록 하여 웹상에서 설계도면 정보유출을 목적으로 하는 사용자가 설계도면을 변경할 수 있는 가능성을 제거하였다. 'PDF(Portable Document Format)'는 설계도면 파일에 비밀번호를 설정하여 설계도면 정보를 전송할 수 있는 방법이다.

그러나 이러한 방법은 설계도면 정보를 보호하기 위한 목적으로 개발된 것이 아니라 설계도면 정보공유 와 함께 이에 대한 무결성(integrity)을 유지하기 위하여 개발된 것이기 때문에 제3의 사용자가 비밀번호를 알게 되었을 경우 쉽게 유출될 수 있는 가능성이 있다. 또한 파일에 대한 접근만을 단순히 제어하기 때문에 불법복제 방지, 사용권한 제어, 보존연한 제어 및 사용 내역관리에 대한 추적 등과 같이 설계도면 유출방지를 위한 보호기능을 수행할 수 없다[2].

3. 작업영역 기반 보안기술 개발

다양한 파일형식으로 구성된 설계도면은 임시파일 형태에서부터 파일형식에 따라 암(복)호화를 수행하여야 할 뿐만 아니라(1:N), 파일들 사이에 선행 연결관계를 지속적으로 관리하여야 하기 때문에 처리속도 및 정확성의 문제가 발생된다. 따라서 설계도면 및 개발 소스코드(source code) 등은 단순히 몇 개의 파일을 암호화하는 것만으로 보호될 수 없다. 따라서 사용자의 작업환경을 그대로 유지하면서 파일형식과 관계없이 임시파일의 생성에서부터 폐기에 이르기까지 전 과정에서 중요정보를 보호할 수 있는 기술개발이 필요하다[1].

본 연구에서는 가상보안 디스크(Virtual Secure Disk)를 생성하고 보안이 요구되는 설계 또는 개발 업무를 진행하면서 인가된 응용 프로그램의 모든 작업결과를 가상보안 디스크 내에만 저장가능하게 하고, 인가되지 않은 다른 응용 프로그램은 가상보안 디스크에 접근하지 못하도록 하는 기술을 개발하였다. 여기에서의 가상보안 디스크는 인가된 사용자 및 응용프로그램이외에서는 사용할 수 없도록 암호화되어 관리되는 가상 파일시스템이다.

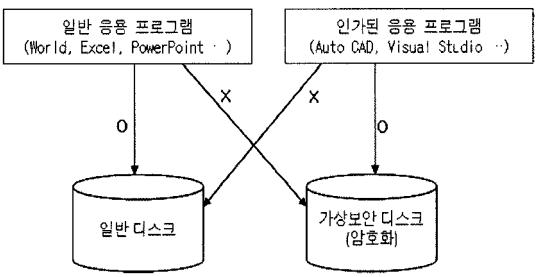
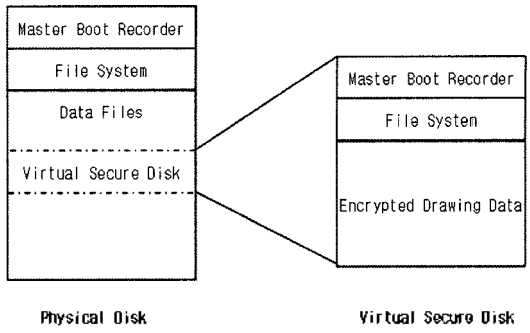


Fig. 2. 작업영역 기반 설계도면 보안방법(응용 프로그램 제어).

3.1 가상보안 디스크 생성

가상보안 디스크는 물리적으로는 하나의 파일이나 운영체제 상에서는 하나의 디스크 드라이브로 인식되는 디스크 형태로 존재한다.

사용자가 가상보안 디스크 설치를 명령하면 일반적인 하드디스크 내 일정공간을 파일형태로 점유하여 가상디스크 볼륨을 생성시킨 다음, 이에 해당하는 정보(디스크의 물리적인 위치, 디스크의 분할 등)를 참고하여 가상보안 디스크 드라이버를 만든다. 이러한 가상보안 디스크 드라이버는 파일을 관리하는 규칙을 정리한 파일 시스템과 연동하면서 새로운 디스크로 인식된다.



※ Master Boot Recorder: 디스크 크기 및 섹터 정보
File Allocation Table: 파일들의 주소 정보

Fig. 3. 가상보안 디스크 논리구조.

사용자의 관점에서는 접근이 제한되는 부분만을 제외하고는 일반 드라이브와 동일하게 동작하기 때문에 업무환경에 변함이 없게 된다.

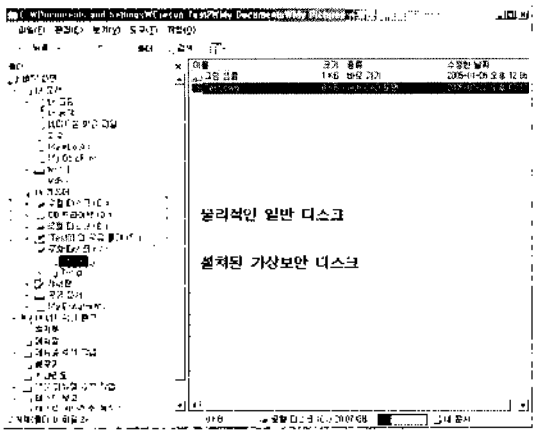


Fig. 4. 가상보안 디스크 생성.

3.2 응용 프로그램 접근제어

생성된 가상보안 디스크를 기준으로 보안정책에 따라 사전에 인가된 응용 프로그램(CAD 프로그램, 개발 프로그램 등)에서 수행되는 모든 정보는 이 디스크로 쓰기(저장)가 가능하며, 일반 디스크로의 쓰기는 불가능하게 한다. 반면에 인가되지 않은 응용 프로그램은 가상보안 디스크로의 읽기나 쓰기작업은 모두 불가능하게 한다.

가상보안 디스크로 파일을 저장할 할 경우에는 API 후킹(Application Programming Interface Hooking) 기술과 시스템 서비스 테이블 후킹(System Service Table Hooking) 기술을 동시에 사용하여 사용자 및

응용 프로그램의 접근을 제어한다. 여기서의 후킹 기술이란 응용 프로그램이 시작되기 전에 사용자가 제어 권을 가로채어 사용자가 정의한 작업을 먼저 실행한 다음 제어를 다시 응용 프로그램에게 넘기는 기술을 의미한다[5,6].

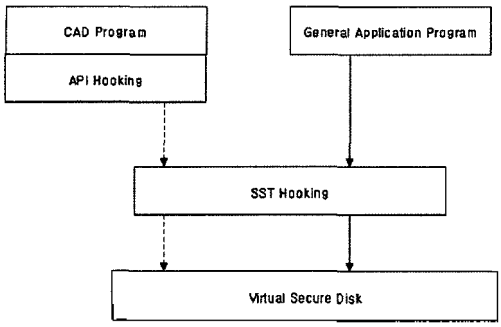


Fig. 5. 응용 프로그램 제어를 통한 가상보안 디스크 접근 방법.

API 후킹기술은 사용자 수준(User Level)에서 가상보안 디스크로 접근이 허용된 응용 프로그램을 제어하기 위하여 사용된다.

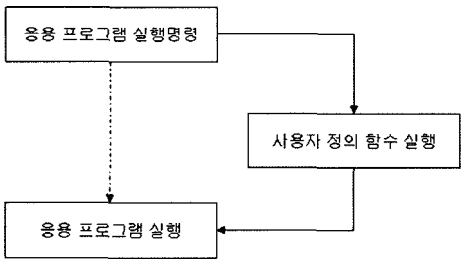


Fig. 6. API 후킹 기술.

그러나 일반적인 응용 프로그램에 대한 가상보안 디스크로의 접근제어를 위하여 사용자가 설치한 응용 프로그램들을 대상으로 API 후킹기술을 모두 적용할 수 없기 때문에 응용 프로그램이 반드시 거치게 되는 시스템 서비스 테이블을 후킹함으로써 시스템 수준(Kernel Level)에서 가상보안 디스크의 접근을 제어한다.

일반적인 윈도우 운영체제 환경에서 응용 프로그램의 실행을 위하여 필요한 사용자 수준의 함수가 호출되면 운영체제는 시스템 서비스 테이블(System Service Table)에서 정의된 사용자 수준의 호출 함수에 대응하는 시스템 수준(System Level)의 함수의 주소를 찾아서 포인터(Pointer)로 연결한다.

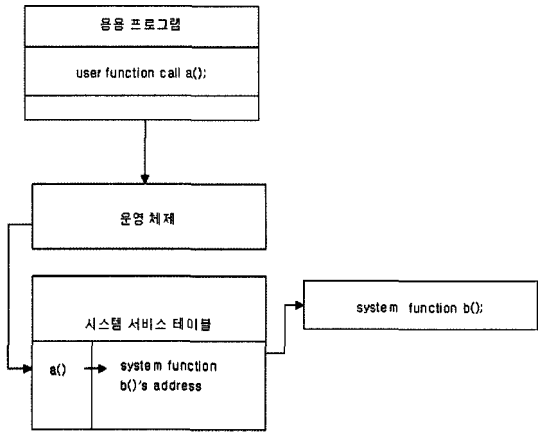


Fig. 7. 시스템 서비스 테이블 후킹기술.

예를 들어, 일반적인 응용 프로그램에서 파일을 열기 위해서는 'CreateFile( )'이라는 Win32 API 함수를 사용한다. 이사용자 수준 함수는 시스템 수준에서는 'Kernel32.dll'에 속해 있는 기본적인 함수로 구현되는데, 응용 프로그램으로부터 사용자 수준의 함수 'CreateFile( )'에 대응하여 운영체제는 'NtCreateFile( )'을 거쳐 시스템 서비스 테이블에 정의된 시스템 수준(System Level)의 함수 'ZwCreateFile( )'을 제공하게 된다.

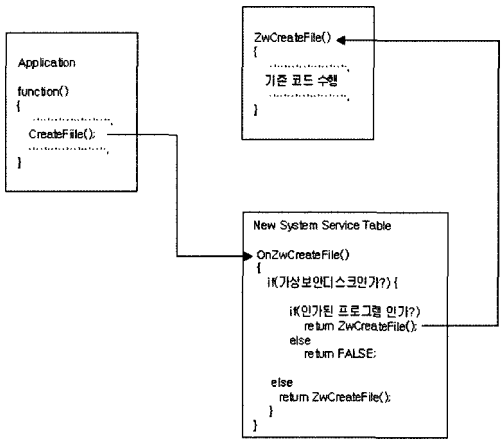


Fig. 8. 시스템 서비스 테이블 후킹기술 사례.

3.3 가상보안디스크 내 설계도면 암(복)호화

가상보안 디스크에 대한 입출력 정보를 그대로 저장하게 되면, 이 디스크가 유출되었을 때 하나의 파일로 간주되어 일반적인 파일 시스템을 사용하여 읽을 수 있는 위험성이 있다. 따라서 가상보안디스크에 관

한 입출력 정보를 암(복)호화하여 관리하여야 한다[7].

일반적으로 중앙처리장치(CPU)의 연산속도에 비하여 디스크 입출력 속도는 현저하게 느리기 때문에 디스크 입출력 작업이 완료될 때까지 중앙처리장치는 대기상태(idle status)에서 기다리게 된다. 이를 고려하여 본 연구에서는 중앙처리장치가 디스크 입출력을 기다리는 대기시간(idle time)동안 암(복)호화를 수행할 수 있도록 가상보안디스크로 입출력되는 모든 설계도면은 섹터단위로 암(복)호화를 수행함으로써 암(복)호화 속도가 디스크 입출력 처리속도보다 작게 되어 시간지연문제가 발생되지 않는다.

이와 같이 본 연구에서 제시한 방법은 보안적용 시점 및 대상에서부터 보안방식, 암호화방식, 지원파일형식 등에 이르기까지 파일단위 보안방법과 차이점을 가지고 있다. 먼저 보안적용 시점 및 대상에 있어서 파일단위의 보안방법은 임시파일의 형태를 거쳐 작업파일을 열고 처음으로 저장하는 시점부터 적용이 되지만, 작업영역 기반 보안방법은 인가된 응용 프로그램을 통해서 임시파일의 생성경로를 조정하여 작업파일이 작성되는 시점에서부터 보안구간이 설정된다.

보안방식에 있어서는 파일단위의 보안방식은 하나의 통일된 파일을 형식에 대하여 암호화를 진행하지만, 작업영역 기반의 보안방식은 파일형식에 관계없이 모든 파일형식을 특정 디스크에 저장함으로써 자동암호화 한다.

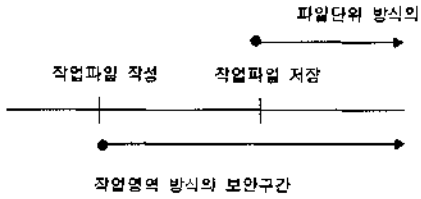


Fig. 9. 보안방식별 보안구간 범위.

마지막으로 파일단위의 보안방식은 특정파일의 구조를 분석하여 암호화를 진행하기 때문에 파일형식에 영향을 받지만, 작업영역 기반방식은 다양한 파일형식을 취급하는 응용 프로그램에 대하여 접근제어를 진행하기 때문에 지원하는 파일형식과는 무관하다(실험 대상 프로그램: Auto CAD, Pro Engineer, CATIA, Matlab, Solid Edge, MS Visio, Acrobat Distiller, Solid Works, Photoshop, Illustrator 등).

3.4 설계도면 외부 반(출)입 통제

일반적으로 사용자 컴퓨터에서 외부로의 설계도면 반출은 이동저장장치, 네트워크 등을 통하여 이루어진다. 본 연구에서는 외부 사용자에게 설계도면을 반출할 때에는 이를 위한 보안 탐색기를 별도로 개발하여 사용한다. 윈도우 운영체제에서 기본적으로 제공하는 윈도우 탐색기(Windows Explorer)는 가상보안 디스크로의 접근이 불가능한 응용 프로그램이기 때문에 가상보안 디스크로의 접근을 통한 중요정보의 반(출)입을 위해서 별도로 개발되었다.

보안 탐색기는 가상 디스크에 저장된 중요정보를 반출하기 위하여 반출사용자, 반출대상, 유효기간, 작업권한(읽기, 수정, 인쇄 가능여부 등) 등을 포함한 반출용 파일을 별도로 생성하여 전달함으로써 다양한 유출경로로 인하여 발생할 수 있는 보안 취약점을 해결하였다. 반출용 파일에는 수신자의 고유정보를 함께 이 정보와 동일한 정보를 가진 수신자만이 수신자의 가상보안 디스크에서 반출용 파일을 복호화하여 사용할 수 있게 된다.

4. 가상보안디스크 적용사례

개발된 기술에 대한 적용가능성을 살펴보기 위하여 국내 D 제조회사에 설치하여 보안성을 검증하였다. 설치된 사용자 컴퓨터 환경의 운영체제는 'Windows XP'이며 도면 설계프로그램은 'Auto CAD 2005'를 사용하면서 일반적인 도면설계 작성업무과정에 따라 테스트를 진행하였다.

사용자가 로그인을 하게 되면 기업 내 보안정책에 따라 사용자에게 부여된 권한이 기존의 파일시스템과 연동되어 사용자 컴퓨터에 가상보안 디스크를 생성한다. 사용자는 도면 설계 프로그램을 실행하여 계획된 작업을 진행한다. 사용자가 작업을 마쳤을 때 도면 설계프로그램에서 진행된 작업을 저장하기 위하여 일반

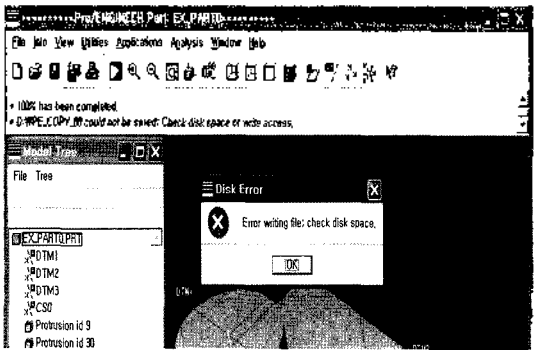


Fig. 10. 도면 설계프로그램에서 일반 디스크에 파일저장을 시도.

디스크로의 저장을 시도하는 경우에는 저장할 수 없다는 내용의 경고메시지와 가상보안 디스크로의 저장을 안내한다.

이와 반대로 일반 응용프로그램(Note Pad)에서 진행된 작업을 가상보안 디스크로 저장하려 할 경우에도 저장할 수 없다는 내용의 경고메시지 출력과 함께 일반 디스크로의 저장을 안내하게 된다.

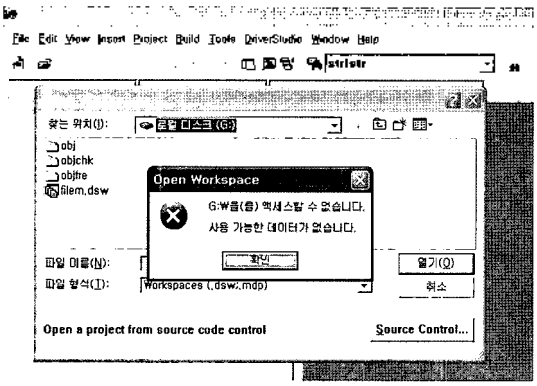


Fig. 11. 일반 프로그램에서 가상보안 디스크에 저장을 시도.

만약에 사용자 작성한 설계도면 파일을 내부나 외부로 반출할 경우에는 보안 탐색기를 사용하여 외부 사용자의 정보와 함께 전달방법, 유효기간 등을 선택하여 반출파일을 생성한다. 이때 파일반출에 대한 승인은 사전에 정해진 기업 내 보안정책에 따라 결정되며 사고를 대비하여 로그를 별도로 기록한다.

이와 같이 설계도면 파일의 특성에 적합한 작업영역 보안방식의 가상보안디스크를 설치함으로써 기업 내 내부 사용자 관리는 물론 외부 사용자에 대한 설계도면 통제가 가능함을 확인하였다.

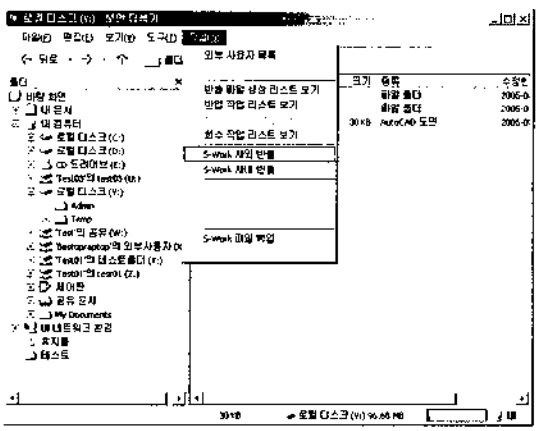


Fig. 12. 보안 탐색기를 사용하여 설계도면 반출.

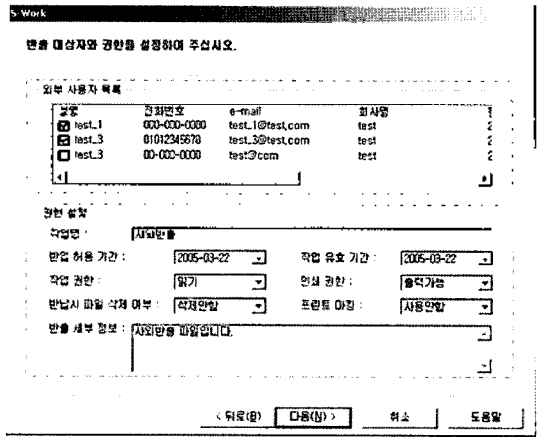


Fig. 13. 설계도면을 전달받을 사용자와 권한 설정.

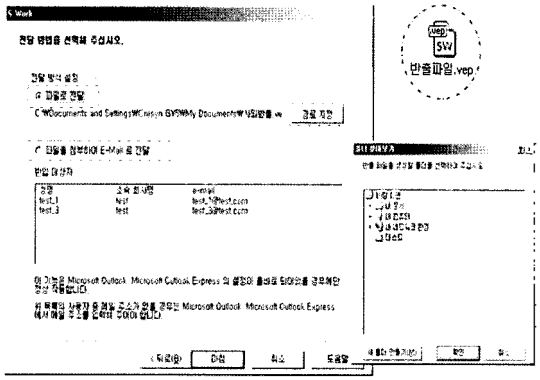


Fig. 14. 설계도면을 전달할 방법 선택.

5. 결 론

최근 기업 내 내부 사용자가 설계도면을 경쟁회사나 다른 국가 등으로 유출시키는 보안사고가 급격히 증가함에 따라 내부 사용자에 의한 정보유출 방지기술이 개발되고 있다. 그러나 기존에 개발된 내부 사용자에 의한 정보유출 방지기술은 정보를 파일단위로 암호화하여 관리하기 때문에 다양한 파일형식들의 집합으로 구성된 설계도면은 확장자에 따라 파일들을 압(복)호화하고, 이들 사이의 선행 연결을 별도로 관리하여야하여야 하기 때문에 보안을 위한 작업의 처리속도 및 정확성 등의 문제로 인하여 적용이 불가능하다.

이에 따라 본 연구에서는 설계도면 정보가 내부 및 외부 사용자에 의하여 불법적으로 유출되는 사고를 방지할 수 있도록 작업영역 기반의 보안기술을 개발하였다. 그 결과 API 후킹 기술과 시스템 서비스 테

이블 후킹 기술을 응용하여 사용자 및 응용 프로그램에 따라 특정 저장 장소로의 접근을 통제(가상보안 디스크)하고, 설계도면 파일을 섹터단위로 암(복)호화하여 저장하고 관리하는 작업영역 기반 보안기술을 개발하였다.

개발된 기술은 파일단위 보안방법의 선행기술과 비교하여 보안적용 시점 및 대상에서부터 보안방식, 암호화방식, 지원파일형식 등의 측면에서 향상된 결과를 얻을 수 있었다.

Table 1. 설계도면 보안방식의 비교

구 분	파일단위 보안방식	작업영역 기반 보안방식
보안적용 시점 및 대상	작업이 완료된 특정파일	작업환경 전 구간에 대한 모든 파일(생성, 사용, 공유, 폐기)
보안 방식	특정 파일의 암호화를 통한 접근권한 제어	설계 작업으로 생성되는 모든 파일에 대하여 암호화를 통한 접근권한 제어
암호화 방식	블록 단위 암호화	섹터 단위 암호화
암호화로 인한 파일 입출력속도	속도 변화 있음	전혀 변화 없음
지원 파일 형식	특정파일 형식	파일형식과 무관

개발된 기술의 적용가능성과 보안성을 검증하기 위하여 국내 제조 기업에 직접 설치하여 적용한 결과 기업 내 설계도면 정보를 안전하게 보안할 뿐만 아니라, 별도로 개발한 보안 탐색기의 반출 기능을 사용하여 외부 사용자의 부분별한 설계도면 사용도 동시에 제어할 수 있게 되었다.

본 연구를 통하여 개발된 기술은 기존의 일반 디스크를 물리적으로 분할하지 않고 현재의 운영체제에 의해 동작하는 시스템에서 별도의 가상디스크와 이에 따른 파일시스템을 통하여 새로운 드라이브로써 관리됨으로써, 드라이브에 저장된 중요정보를 사용하고자 할 경우 인가된 사용자와 응용 프로그램에 대해서만 접근이 허용된다. 이 기술은 모든 중요정보를 중앙서버에 저장하고 있는 'Thin Client' 컴퓨팅 환경과 이와 반대로 사용자 컴퓨터 시스템에 모든 중요정보를 저장하고 있는 'Fat Client' 컴퓨팅 환경의 장점들을 각각 취합하여 중요정보를 중앙서버와 사용자 컴퓨터 시스템에서 공유하고 있는 컴퓨팅 환경(중앙서버에서는 최소한의 작업을 수행하며 공용 파일이나 프로그램을 저장하고, 개인용 컴퓨터 시스템에서 대부분의 모든 작업을 수행하나 정보의 중요도에 따라 개인용 저장 공간과 조직용 저장 공간을 분리하여 관리하는 컴퓨팅 환경)을 위한 정보보호 기술개발에 적용될 수 있을것으로 기대된다[8].

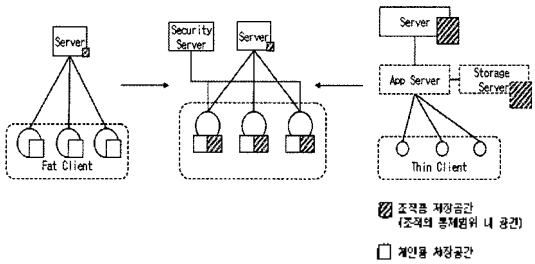


Fig. 14. 컴퓨팅 환경의 변화(사용자 컴퓨터 시스템 내 조직용 저장 공간 설치).

감사의 글

본 연구는 중소기업청 '중소기업기술혁신개발사업'의 지원으로 수행되었으며, 이에 감사드립니다.

참고문헌

1. 염근철, 이세정, "다양한 소프트웨어 개발환경에서의 최적설계 프레임 웍", CAD/CAM학회논문지, 제10권, 제5호, 2005.
2. 이기동, 김준우, "디지털 콘텐츠 정보보호를 위한 저작권 관리시스템 설계 및 구현", 경영정보학연구, 제13권, 제4호, 2003.
3. 정연찬, 박준철, "CAD/CAM 응용 소프트웨어 개발을 위한 형상 커널 개발", 제6권, 제4호, 2001.
4. Marianthi Theoharidou, Spyros Kokolakis Maria Karyda, Evangelos Kiountouzis, "The Insider Threat to Information Systems and the Effectiveness of ISO17799", *Computer & Security*, Vol. 24, 2005.
5. Green, R., "CAD Manager: Drawing Security", Cadalyst, 2005.
6. Basie Von Solms, "Information Security Governance: COBIT or ISO 17799 or Both?", *Computer & Security*, Vol. 24, 2005.
7. Edward N. Deker and Joseph M. Newcomer, "Developing Windows NT Device Drivers: A Programmer's Handbook", Addison-Wesley, 1999.
8. Rajeev Nagar, "Windows NT File System Internals : A Developer's Guide" O'Reilly & Associates, 1997.
9. Chechanowicz, Z., "Risk Analysis: Requirements, Conflicts and Problems", *Computer & Security*, Vol. 16, 1997.
10. Eloff, J. and M. Eloff, "Information Security Management - A New Paradigm", Proceedings of SAIC-

SIT, 2003.
11. Lee, Y. H. and Hwang, D. J., "Design and Implementation of Agent Based Dynamic Digital Rights Management", *Journal of Information Processing Association*, D. Vol. 8D, No. 5, October 2001, pp. 613-622.
12. Otwell, K. and B. Aldridge, "The Role of Vulnerability in Risk Management", IEEE Proceedings of the 5th Annual Computer Security Applicant Conference, pp. 32-38, 1989.

장 항 배

1997년 2월 중앙대학교 컴퓨터공학과 학사
1999년 8월 중앙대학교 컴퓨터공학과 석사
2006년 2월 연세대학교 정보대학원 박사
2003년 3월~현재 소프트캠프(주) 정보보안기술연구소 책임연구원

관심분야: 정보보호, 유비쿼터스 컴퓨팅, 건설정보화, 이 비즈니스 전략

이 호 신

1980년 2월 서울대학교 토목공학과 학사
1981년 8월 스탠포드대학교(캘리포니아) 토목공학과 석사
1985년 12월 텍사스 주립대학교(오스틴) 토목공학과 박사
1986년 10월~1988년 7월 영 타운 주립대학교 토목공학과 교수
1988년 8월~1991년 12월 워싱턴 주립대학교 토목공학과 교수
1992년 1월~1999년 6월 유타 주립대학교 토목공학과 교수
1999년 7월~현재 아이오와 주립대학교 토목공학과 교수

관심분야: 건설 정보화, 정보보호, 도로 설계 및 포장기술 연구, 사회간접자본 관리시스템