파일유출 방지를 위한 저장장치 제어기법에 대한 연구

최주호* · 류성열**

요 약

클라이언트에 저장된 파일이나 도면등의 자료가 외부로 유출되는 것을 방지하기 위해서는 파일을 생성한 자신도 관리자의 허락 없이는 저장장치로 파일을 저장/복사할 수 없는 제어가 필요하다. 저장장치 제어를 위하여 저장장치를 디바이스와 드라이브로 인식할 수 있어야 하고, 저장장치의 사용을 제어하기 위한 제어값 설정과 저장프로세스를 후킹하여 파일의 저장을 제한 할 수 있는 방법을 연구한다. 이를 수행하기 위하여 파일시스템의 Win32 API함수를 후킹하여 해당 드라이브에 설정된 제어값을 참조하고 파일의 저장프로세스를 제어하는 기법을 제안하였다. 제안한 기법이 제어가 설정된 저장장치에 파일을 복사/저장하면 쓰기가 금지되어 제어가 수행됨을 실험으로 확인하였다.

A Study of Storage Device Control Method for File Outflow Protecting

Joo-ho Choi* · Sung-yul Rhew**

ABSTRACT

The files of intellectual property on computer systems have increasingly been exposed to such threats that they can be flowed out by internal users or outer attacks through the network.

The File Outflow Protection System detects file outflow when users not only copy files on client computers into storage devices, but also print them. This Protection system has been designed to Win32 API hooking by I/O Manager in kernel level if files are flowed out by copying. As a result, the monitoring system has exactly detected file outflows, which is proved through testing.

* (주)디지탈센스

** 숭실대학교 정보과학대학 컴퓨터학부

1. 서 론

정보보안의 핵심은 정보의 중요자산을 외부로부터 침입/파괴/변조를 방지하는 부분과 외부/내부 사용자에 의해 중요 정보의 유출을 방지하는 부분으로 구분할 수 있다. 컴퓨터 내부의 정보는 서버 및 컴퓨터 등이 고도화되고, 저장장치는 소형화와 대용량화되어 디스켓이나 CD-RW, 이동저장매체 등을 통하여 내부정보의 복제, 유출, 인쇄가 용이하게 되었으며, 인터넷과 네트워크는 고속화되어 다량의 데이터를 쉽게 전송할 수 있어 보다 안전한 보호 장치 및 관리시스템이 요구되고 있다[1].

정보보호의 대상을 서버와 클라이언트로 구분할 수 있으며, 서버에 대한 보안은 접근 권한이 없는 사용자가 시스템에 접근하여 시스템의 정보를 절취, 훼손하는 위협으로부터 시스템을 보호하는 '시스템 보안'과 정보가 통신망을 통하여 전송되는 과정에서 도청, 송수신부정, 수신자의 문서변경, 문서훼손 등의 위협으로부터 정보를 보호하는 '네트워크 보안'[2], 파일에 대한 접근과 변경 및 훼손, 유출 등의 위협으로부터 보호하는 '파일보안'으로 세분할 수 있다. 시스템에 대한 위협요소는 인터넷과 내부 네트워크의 취약점을 이용하여 시스템 내부를 대상으로 공격하는 방법, 리모트에서 시스템을 공격하는 방법, 관리자 계정을 이용한 공격 방법, 백도어 프로그램을 이용한 정보유출 등의 방법이 있다[3]. 시스템 보안은 이러한 위협으로부터 보호하기 위한 방법으로 시스템에 접근을 제한하기 위한 사용자 인증, 시스템 접근에 대한 모니터링, 파일시스템의 보호, 네트워크 파일 공유에 대한 보호, 레지스트리 변경에 대한 접근제한 방법 등이 제안되고 있다[4-7]. 네트워크보안에는 방화벽, 침입탐지 및 방지, VPN(Virtual Private Network)등을 이용하여 보안을 유지한다[8]. 클라이언트에서 문서의 작성이나 도면의 작업등이 이루어지고 있어 개인 컴퓨터내의 파일에 대한 보안이 중요해지고 있다. 기업에서는 기술 경쟁력이 심화되고 산업스파이의 활동이 증가하여 내부 사용자에 의해 클라이언트내의 파일이 외부로 유출되는 것을 방지할 필요성이 증가하고 있다. 클라이언트에 대한 보호는 바이러스백신이나 개인방화벽, 파일암호화 등의 방법을 사용하고 있으나 이러한 방법은 내부 사용자에 의해서 파일이 외부로 유출되는 것을 방지하는 기능은 제공하지 못한다.

본 연구는 Windows 환경에서 클라이언트에 저장된 파일에 대한 보호방법으로 파일을 생성한 자신도 관리자의 허락없이는 저장장치로 파일을 복사/저장하여 외부로 유출을 방지하기 위한 저장장치 제어 방법을 설계하고 구현한다. 이를 위하여 저장장치의 제어 설정을 위하여 저장장치를 드라이브와 디바이스로 인식하는 방법과 디바이스에 대해 파일의 저장/복사를 제한할 수 있는 제어값 설정과 파일을 저장하는 시점을 후킹(Hooking)하여 제어를 수행하는 방법을 연구하였다. 파일을 보호하는 방법으로 접근권한 부여 방법과 DRM (Digital Right Management)에 대하여 조사하였으며 유출방지를 위하여 요소 기술인 파일시스템과 디바이스 드라이버, 후킹 등에 대해서 관련 논문과 기술서적을 조사하였다.

클라이언트에서 파일과 도면의 생성 및 저장작업이 많이 이루어지는 환경에서 파일의 유출 위험성이 증가하고 있어 저장장치의 제어로 파일유출을 방지할 수 방법은 내부 보안강화에 크게 기여할 것이다.

2. 관련 연구

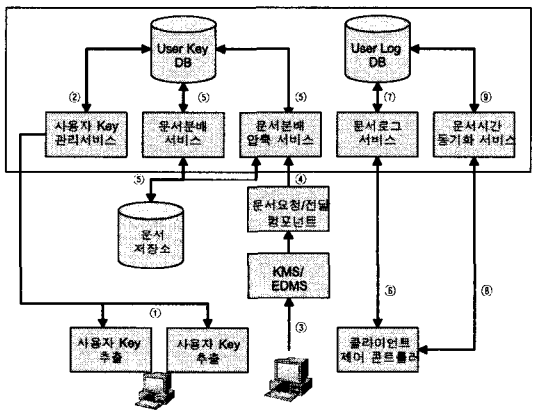
2.1 파일의 접근제한 방법

파일의 접근이나 사용에 대한 보안 방법은 일반적으로 파일에 대한 접근제한과 암호화를 이용하여 보안을 유지하고 있다[9]. 파일에 대한 접근 제

한은 운영체제에서 제공하는 기능을 이용하는 방법과 응용프로그램을 이용하는 방법이 있다. 이들 방법은 파일과 디렉토리에 대해 Delete, Open, Read, Rename, Write동작을 시스템 레벨(System Level)에서 판단하여 권한을 부여 받은 사용자에게 권한을 허용하는 방법이다[10]. 접근제어 기술은 CL(Capability List), SL(Security Label), ACL (Access Control List)로 나누며 CL은 명시된 객체를 규정된 방법으로 접근하도록 권한을 부여받은 사용자가 소요할 수 있는 하나의 접근허가 목록이고, SL은 보안 레이블을 사용하여 다중등급 접근제어를 사용하는 방법이다. ACL은 모든 객체에 대한 접근제한이 적용되어 누가 어떤 객체에 접근할 수 있는지를 통제한다[6]. 파일에 대한 접근제한 방법은 사용 권한에 따라 파일을 읽거나 수정, 저장 등이 가능하여 접근을 통제할 수 있으나 파일에 대한 유출을 방지하는 기능은 제공하지 않는다.

2.2 서버의 파일 보호 방법

기업의 서버에 저장되어 있는 파일을 보호하는 방법으로 DRM기술을 이용한 제품이 개발되고 있으며 이를 이용한 보안 방법을 제안[11, 12]하고 있어 살펴본다. DRM은 디지털 컨텐츠가 생성될 때부터 배포, 이용될 때까지 전 과정의 생명주기(Life cycle)에 걸쳐 컨텐츠의 사용 및 사용관리를 위한 소프트웨어와 하드웨어 기술 및 서비스들의 모임으로 정의하고 있으며 이는 크게 '저작권 관리 기술'과 '저작권 보호기술'로 구분한다[13]. 저작권 관리기술은 세계적으로 통일된 일련의 관리체계를 마련하기 위한 것으로 크게 식별(identification), 기술(description) 및 관련 규칙을 설정(rules-setting)하는 기능으로 구분할 수 있다. 저작권 보호기술이란 저작권의 식별, 설명, 규칙설정이 정해진 뒤 그에 따른 규칙이 실행되는 것을 보장하기 위한 방법으로 컨텐츠를 보호하는 기술이다. 컨텐츠를 보호하는 요소기술은 크게 컨텐츠의 암호화, 위·변조방지(Tamper-proofing), 디지털 워터마킹(watermarking) 및 디지털 지문날인(fingerprinting) 기술로 구분할 수 있다[13]. DRM기술을 적용하여 KMS(Knowledge Management System)과 EDMS (Electronic Data Management System)의 문서유출방지를 위해 제안한 DRM의 구조는 (그림 1)과 같다[12].



(그림 1) KMS에 적용한 DRM시스템의 구조

기업 내에서 DRM 기술은 컴퓨터 내부의 문서파일, 텍스트나 이미지형태의 Web Contents, 프린터로 출력 시 워터마킹을 이용한 출력물 보안, e-mail 보안 등에 적용하여 보안을 강화하고 있으며 문서의 외부 유출 시 사용금지, 문서별 다양한 권한 설정 및 제어, 화면 캡쳐 방지, 로그관리, 문서 유효기간 관리, 워터마킹을 이용한 문서의 출력물 추적 등의 기능을 제공하고 있다[12, 14]. 이러한 기능을 제공하기 위하여 DRM을 구성하는 가장 기본적인 핵심요소는 User, Content, Permission, Condition이다[12]. User는 부여된 Permission과 Condition에 따라 Content를 이용할 주체이며, Contents는 지적자산의 가치가 있는 정보 단위이며 허가되지 않은 사용자로부터 보호하여야 할 대상이다. Content의 이용 권리는 Content별로 정해

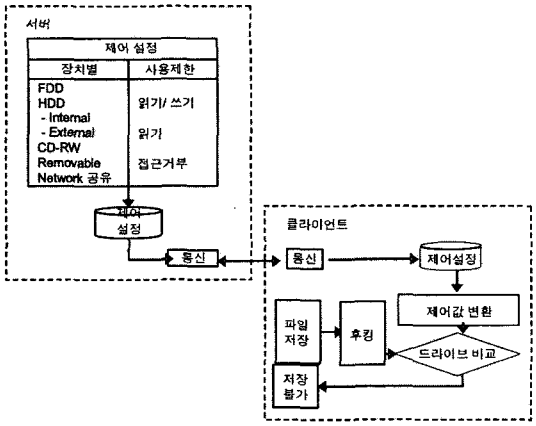
진 Permission에 의해 결정된다. Permission은 사용 및 접근에 대한 허용여부이며 Condition은 Permission이 수행되기 위한 요구조건 및 제한요소를 포함한다.

DRM기술을 이용한 문서보안 방법은 특정한 환경에서 파일에 대한 접근을 제한하고 파일을 암호화하여 정보의 노출을 방지하는 방법은 적합하나 파일의 유출을 방지하는 기능은 제공하지 못한다. Content의 위치가 파일서버나 웹서버에 저장되어 파일을 Download받는 경우에 효과적으로 적용할 수 있으나 자신이 생성한 파일에 대해 유출을 방지할 수 있는 기능은 제공하지 않는다. DRM기술은 파일의 생성자나 관리자가 신규 생성된 Content에 대해 사용자별, 파일별로 Permission을 부여하는 작업과 파일에 대해 사용을 통제하기 위해서 읽기, 쓰기, 저장, 출력 등의 Condition을 설정하는 작업을 수행하여야만 설정된 권한에 따라 문서의 사용을 제한할 수 있다. DRM기술을 적용한 파일이나 문서보안 방법은 권한을 부여하는 과정이 필요하고, 자신이 생성한 문서에는 권한을 부여하지 않고 외부로 파일을 유출 시킬 수 있는 방법이 있어 클라이언트에서 생성한 문서에 대한 보안방법으로 충분하지 못하여 파일의 유출 방지를 위해서는 다른 방법에 대한 연구가 필요하다.

3. 파일유출 방지를 위한 디바이스 제어 기법

3.1 파일유출 방지 방법의 환경

본 논문에서 제안하는 파일유출 방법은 Windows 2000과 XP 환경에서 작동되며, 서버에서 저장장치에 대해 제어를 설정하여 클라이언트에 전달하면 클라이언트에서 문서를 생성한 자신도 이동저장매체와 네트워크 공유를 통하여 파일을 저장/복사할 수 없어 유출을 방지하는 방법이다.

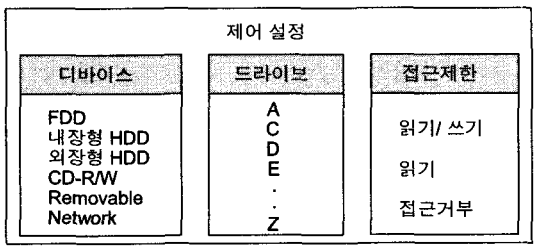


(그림 2) 파일유출 방지 방법의 환경

파일의 유출을 방지하는 방법의 구성은 (그림 2)와 같이 클라이언트/서버 구조로 설계되었다. 서버에서는 저장장치에 제어를 설정하는 기능을 수행하고 클라이언트는 제어신호를 수신하여 문서 사용자가 저장장치에 파일을 저장하는 경우에 제어가 설정된 저장장치인지 비교하여 같으면 저장을 허용하지 않음으로써 파일의 유출을 방지하도록 수행한다.

3.2 제어설정 방법

저장장치를 제어하기 위해서 필요한 사항은 디바이스와 드라이브별로 제어를 설정할 수 있어야 하며 저장장치에 대해서 사용을 제한하는 방법이 필요하다. 저장장치의 제어 대상을 (그림 3)과 같이 '드라이브'와 '디바이스'로 구분하여 제어를 설정한다.



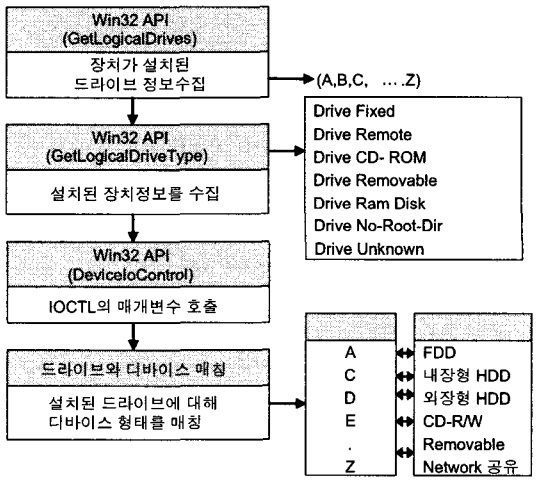
(그림 3) 제어설정 방법

여기에서 '드라이브'는 explorer나 command창에서 설치된 장치(디바이스)를 A, B, C....Z로 표시하는 것이며 '디바이스'는 장치를 기능이나 외형에 의해 일반적으로 분류한 것으로 'FDD', '내장형 HDD', '외장형HDD', 'CD-R/W', 'Removable', '네트워크공유' 등으로 구분한다. 이와 같이 구분하는 것은 드라이브는 Explorer창에서 디바이스가 설치되면 즉시 인지할 수 있으나 설치된 장치가 내장형 HDD, 외장형HDD, CD-R/W, USB와 같이 쉽게 구분할 수 없다는 점이다. 파일을 외부로 유출을 방지하기 위해서는 HDD도 내장형인지 외장형인지 구분되어야 하며 HDD와 CD-R/W, USB등의 장치로 구분되어야 필요한 저장장치만을 선택하여 제어할 수 있기 때문이다. 저장장치가 설치되면 '드라이브'는 장치가 설치되거나 제거 될 때마다 바뀔 수 있으며 현재 설치되지 않은 드라이브에 대해서는 제어를 설정할 수 없는 점이 있다. '디바이스'별로 제어를 설정하면 저장장치가 2개 이상 설치된 경우와 현재 클라이언트에 설치된 저장장치 뿐 만아니라 향후 설치될 저장장치에 대해서도 제어를 일관되게 설정하고 수행할 수 있는 장점이 있다.

저장장치에 대한 접근과 사용을 제한하기 위한 구분은 '읽기/쓰기'(Read & Write), '읽기'(Read Only), '접근거부'(Access Deny)로 나분다. '읽기/쓰기'는 해당 장치에서 파일을 읽기와 쓰기가 가능하며, '읽기'는 읽기는 가능하나 쓰기가 금지되고, '접근거부'는 읽기와 쓰기가 금지된 상태를 말한다. 이와 같이 접근 제한을 구분하는 것은 '읽기'로 설정하면 CD-ROM이나 USB, 외장형 HDD등의 장치에 저장된 프로그램이나 데이터의 읽기가 가능하고 단지 저장만을 제한함으로써 외부로의 유출만을 방지할 수 있으나 '접근거부'로 설정하여 해당 저장장치를 자료의 읽기까지 제한하여 사용의 불편을 줄이고자 한다. 본 논문에서 '제어 설정'이라 함은 저장장치에 '읽기/쓰기' 상태에서 '읽기'나 '접근거부' 상태로 변경하여 파일을 저장하지 못하게 하는 상태를 말한다.

3.3 드라이브와 디바이스의 인식 기법

저장장치에 대해 '드라이브'나 디바이스'별로 제어를 설정하기 위하여 클라이언트에 설치된 저장장치의 '드라이브'가 어떤 '디바이스'인지를 구분하고 일치시키는 과정이 필요하며 처리 절차는 (그림 4)와 같다.



(그림 4) 디바이스/드라이브 인식 절차

드라이브를 인식하기 위하여 Win32 API인 'GetLogicalDrives'의 함수를 후킹하여 A,B,C.....Z까지 논리적으로 디바이스가 설치된 드라이브의 매개변수 값을 구하여 드라이브에 장치가 설치되었는지를 알 수 있다. 드라이브에 어떤 디바이스가 설치되었는지는 'GetLogicalDriveType'의 함수의 매개변수를 이용하여 현재시점에서 설치된 디바이스의 형태를 'Drive Fixed', 'Drive Remote', 'Drive CD-ROM', 'Drive Removable', 'Drive Ram Disk', 'Drive No-Root-Dir', 'Drive Unknown'으로 구분하여 해당하는 디바이스의 매개변수 값을 구한다. 'DeviceIoControl' 함수를 이용하여 'GetlogicalDrive'에서 구한 드라이브 매개변수 값을 'IOCTL'에 대

입하면 'GetLogicalDriveType'의 디바이스 정보를 얻어 설치된 드라이브가 어떤 형태의 디바이스인지를 알 수 있어 매칭시킬 수 있다. 상기의 함수를 계속 후킹하고 있으므로 클라이언트에 외장형 HDD나 CD-R/W, USB등의 디바이스를 설치하거나 제거하게 되면 실시간으로 변경된 드라이브와 디바이스 정보를 수집하며, 현재 설치되지 않은 디바이스나 드라이브에 제어가 설정되어도 파일의 저장시점에 해당 디바이스가 설치되어 있으면 이를 인식하여 제어를 수행할 수 있다. 내장형 HDD와 외장형 HDD가 동시에 2개 이상 설치된 경우에 같은 'Drive Fixed'로 인식되어서 이를 구분하기 위해서는 'DeviceIoControl' 함수의 'DeviceIOCTL-Storage-Query-Property' 매개변수를 이용하며 'Bus-Type'으로 구분한다.

3.4 드라이브 및 디바이스에 제어 설정

서버에서 저장장치에 제어를 설정하면 클라이언트에서 제어를 수행하기 위한 코드값으로 변환하여 저장한다. 이를 처리하는 방법으로 드라이브는 A에서 Z까지 인식되므로 <표 1>과 같이 26개의 필드를 구성하고 해당 드라이브에 제어 설정값을 저장한다. 디바이스에 대한 제어설정 방법은 <표 2>와 같이 FDD : '1', 내장형HDD : '2', 외장형 HDD : '3', CD-R/W : '4', Removable : '5', Network 공유 : '6'으로 구분한다. 접근제한을 위한 코드는 '읽기/쓰기'는 '0', '읽기'는 '1', '접근거부'는 '2'로 설정한다.

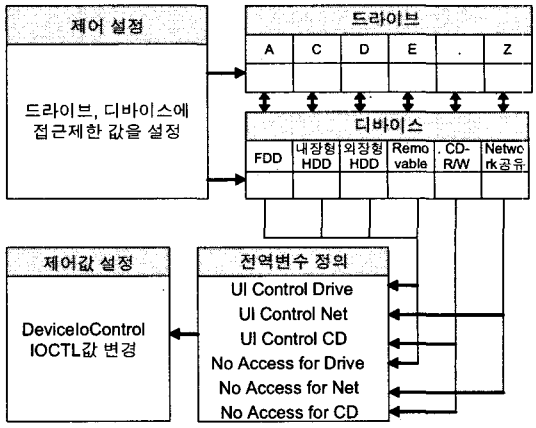
〈표 1〉 드라이브에 대한 제어 설정

드라이브	A	B	C	D	E	.	Z
접근제한 코드							

〈표 2〉 디바이스에 대한 제어 설정

디바이스	FDD	내장형 HDD	외장형HDD	CD-R/W	Removable	Network 공유
접근제한 코드						

서버는 <표 1>, <표 2>의 제어를 설정하고 이를 클라이언트에 소켓통신으로 전송한다. 클라이언트가 네트워크에 연결되지 않은 상태이면 클라이언트가 부팅하여 서버에 접속하여 이를 수신한다. 클라이언트에서 제어값이 설정되는 과정은 (그림 5)와 같다.

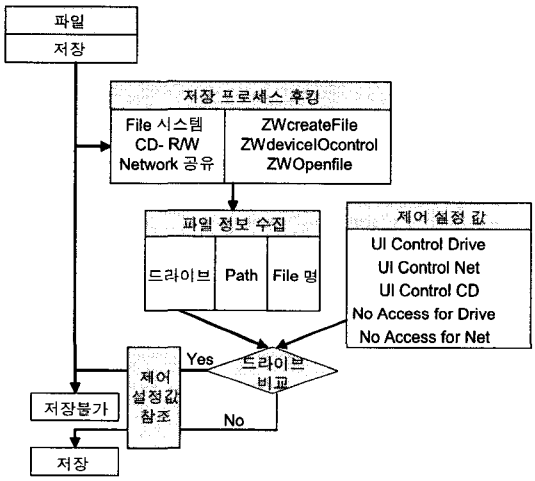


(그림 5) 제어 설정 방법

제어값을 설정하기 위하여 전역변수를 'UI Control Drive', 'UI Control Net', 'UI Control CD', 'No Access for Drive', 'No Access for Net', 'No Access for CD로 정의한다. 이 전역변수는 제어를 설정한 값을 보관하여 현재 설치된 저장장치에 대한 제어와 향후 설치될 장치에 대한 제어를 수행하기 위하여 필요하며 시스템 함수에 제어값을 치환하는데 사용된다. 서버에서 제어가 설정되면 <표 1>의 접근제한 코드를 클라이언트에서 정의한 전역변수에 입력한다. 예를 들어 FDD, 내장형 HDD, 외장형HDD, Removable 장치에 대해 '읽기/쓰기'가 설정되어 있으면 'UI Control Drive'에 (드라이브, 디바이스, 접근제한 코드) 형식으로 입력된다. 전역변수에 입력된 제어 설정값을 디바이스에 관련된 시스템 함수인 'DeviceIoControl' 함수를 호출하여 제어가 설정된 드라이브의 'IOCTL'의 매개변수 값을 '읽기'에 해당하는 '1'이나 '접근거부'에 해당하는 '2'로 변환하여 제어를 설정한다.

3.5 파일의 저장시점에 대한 후킹과 제어 수행

사용자가 파일을 저장하는 작업을 수행하면 전체 과정을 후킹하여 저장하려는 '드라이브'와 '파일정보'를 수집한다. 해당 드라이브에 제어가 설정되었는지 알기 위해 저장프로세스를 후킹하여 저장하려는 드라이브 정보를 추출하고 시스템 함수를 호출하여 이미 제어가 설정되어 있는지를 비교하여 같으면 제어를 수행하며 처리 방법은 (그림 6)과 같다.



(그림 6) 파일의 저장프로세스 후킹과 제어 처리

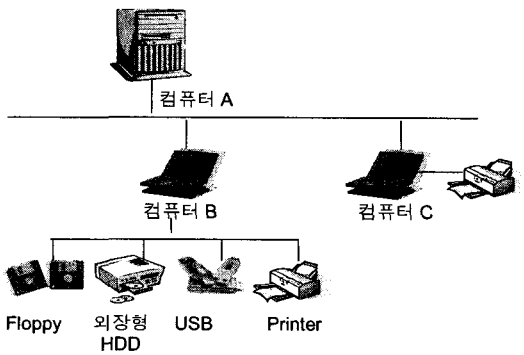
사용자가 파일의 저장하는 작업을 수행하면 해당 프로세스를 후킹하여 저장하고자하는 드라이브에 제어가 설정되어 있으면 파일이 저장되지 않도록 처리하는 과정이 필요하다. 여기에서 후킹하는 함수들은 파일시스템은 'ZwcreateFile', CD-R/W에서 작업은 'ZwdeviceIoControl', 네트워크 공유에 대한 작업은 'ZwOpenFile'이다. 이 함수들을 통하여 파일을 저장하는 시점에서 해당 프로세스의 드라이브, 파일Path, File명에 대한 정보를 수집한다. 후킹한 프로세스로부터 파일을 저장하려는 드라이브 정보를 추출하고 해당 드라이브가 접근 제한이 설정되었는지를 알기 위하여 전역변수에 제어가 설정된 값과 드라이브를 비교한다. 저장 프로세스는 저장작업을 수행하기 위하여 'DeviceIoControl' 함수를 호출하여 'IOCTL' 값을 참조하게 되며 이미 저장할 수 없는 제어값이 설정되어 있어 파일을 저장할 수 없음을 알리는 메시지를 보내고 작업을 종료하게 된다.

4. 시험 및 결과

Windows환경에서 서버에서 저장장치에 제어를 디바이스나 드라이브별로 설정할 수 있어야하며, 클라이언트의 저장장치가 '읽기'나 '접근거부'로 설정되어 있으면 해당 저장장치에 파일의 저장을 시도하여도 수행되지 않아 파일의 유출을 방지할 수 있는지를 확인한다.

4.1 시험 환경

파일의 유출을 방지하기 위한 시험 환경은 (그림 7)과 같이 구성하였으며, '컴퓨터 A'에는 Windows 2000 Server 환경에 서버프로그램을 설치하였고, '컴퓨터 B'는 Windows XP Home Professional, '컴퓨터 C' Windows 2000 Professional 환경에 클라이언트 프로그램을 설치하고 네트워크로 연결하였다. 컴퓨터 B와 C에 FDD, CD-R/W, 외장형 HDD, USB 2.0 저장장치를 설치하였다.



(그림 7) 시험 환경의 구성

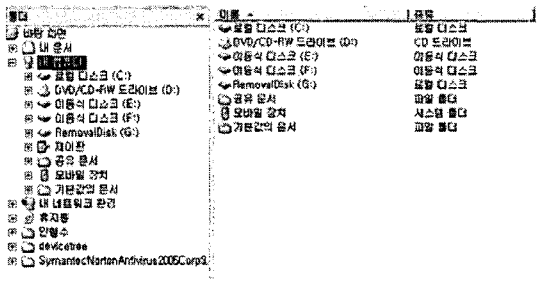
4.2 시험 방법

1) 컴퓨터 A에 서버프로그램을, 컴퓨터 B와 컴퓨터 C에 클라이언트 프로그램을 설치하고 네트워크로 연결한다.
2) 컴퓨터 B에 FDD, 내장형 HDD, CD-R/W, 외장형 HDD, USB를 설치하면 컴퓨터 A에 설치된 서버 프로그램에서 이를 드라이브와 디바이스별로 인식하는지를 확인한다.
3) 컴퓨터 A에 설치된 서버프로그램에서 컴퓨터 B의 외장형 HDD와 USB를 '읽기(Read Only)'와 접근 거부로 설정하고 외장형 HDD와 USB의 파일을 내장형 HDD에 복사하여 저장이 수행되는지를 확인한다. 반대로 내장형 HDD의 파일을 외장형 HDD와 USB에 파일을 복사하여 저장하면 제어가 설정되어 수행되지 않은지를 확인한다.

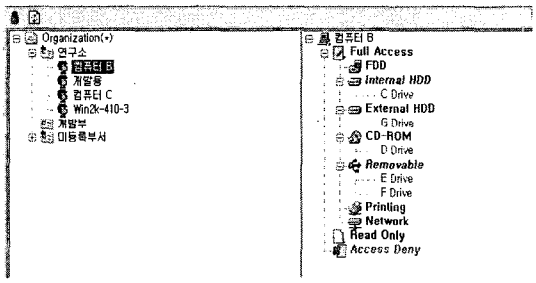
4.3 시험 결과

4.3.1 저장장치의 인식에 대한 시험 및 평가

컴퓨터 B에 설치된 저장장치에 대해 Explorer에 표시된 내용이 (그림 8)이고 서버에 저장장치가 드라이브와 디바이스로 구분되어 인식된 내용이 (그림 9)이다. (그림 8)과 같이 컴퓨터B에 내장형 HDD는 'C'드라이브에 '로컬디스크'로, 외장형 HDD는 'G' 드라이브에 'Removal Disk'로, USB는 'E'와 'F'에 '이동식디스크'로 표시되었다. 서버에서는 (그림 9)와 같이 내장형HDD는 'Internal HDD'와 'C Drive'로, 외장형HDD는 'External HDD'와 'G Drive'로, USB는 'Removable'에 'E Drive'와 'F Drive'로 표시 되었다. 이와 같이 클라이언트에 설치된 저장장치는 정확히 서버에 표시되었으며, 디바이스와 드라이브로 인식할 수 있었다. 따라서 디바이스별로 제어를 설정하게 되면 현재의 설치된 저장장치와 향후에 설치될 저장장치까지 제어를 수행할 수 있다.



(그림 8) 클라이언트 Explorer창에서 장치 설치현황



(그림 9) 서버에서 저장장치 설치 표시 화면

컴퓨터 B와 컴퓨터 C에서 FDD, HDD, 외장형 HDD, USB를 각각 6회 설치하고 각각의 저장장치가 정의한 디바이스로 인식하는지를 측정한 결과는 <표 3>과 같다.

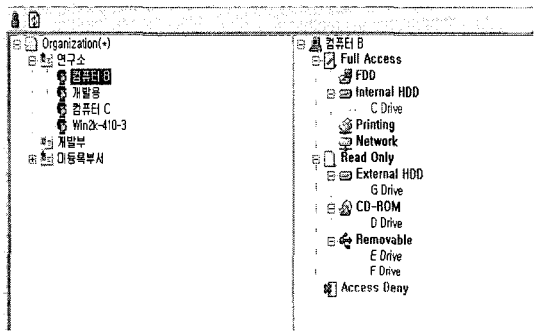
컴퓨터에 드라이브로 인식되는 저장장치가 설치되면 분류된 디바이스 형태로 정확하게 인식됨을 확인하였다.

〈표 3〉 저장장치의 인식

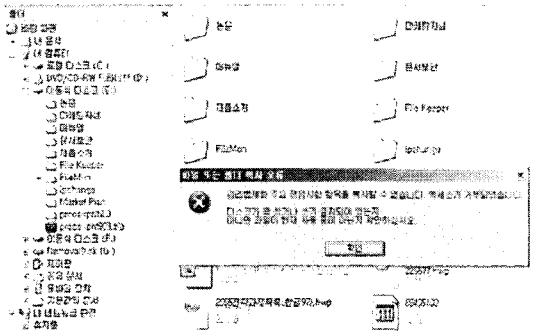
운영체제	시험횟수	정상적으로 인식 횟수				
		FDD	가상드라이브	외장형 HDD	USB	네트워크 공유
Windows XP Pro	30회	6회	6회	6회	6회	6회
Windows 2000	30회	6회	6회	6회	6회	6회

4.3.2 저장장치의 제어 수행에 대한 정확성 시험 및 평가

컴퓨터 B에 설치된 저장장치에 대해 Explorer에 표시된 내용이 서버 프로그램이 설치된 컴퓨터 A에서 컴퓨터 B의 'External HDD', 'CD-ROM', 'Removable'을 (그림 10)과 같이 'Read Only'로 제어를 설정하였다.



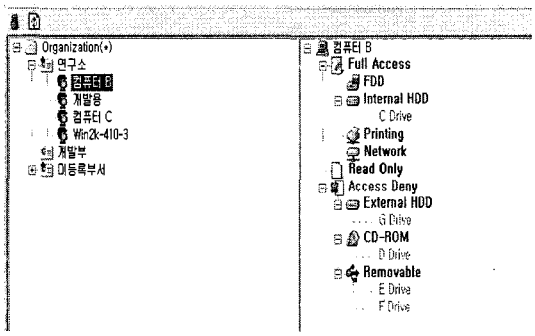
(그림 10) 서버에서 Read Only로 제어 설정 화면



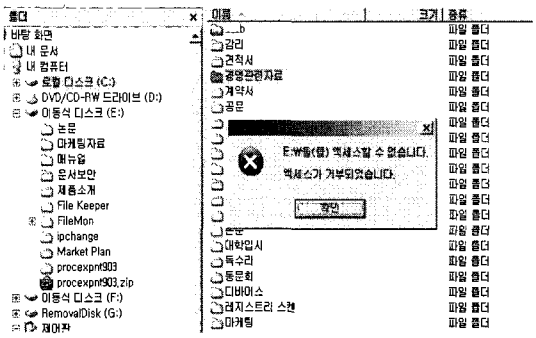
(그림 11) Read Only로 설정된 USB에 파일을 저장

(그림 10)과 같이 USB에 'Read Only'로 설정한 후 USB에 파일의 저장을 시도하면 (그림 11)과 같이 저장 할 수 없음을 알리는 메시지가 표시되고 작업이 종료되었다. 제어가 설정된 외장형 HDD에 파일의 저장을 시도하였지만 결과는 동일하여 설정된 제어 기능이 정상적으로 수행되었다.

서버 프로그램이 설치된 컴퓨터 A에서 컴퓨터 B의 'External HDD', 'CD-ROM', 'Removable'을 (그림 12)와 같이 'Access Deny'로 제어를 설정하였다. (그림 13)과 같이 'C' 드라이브의 파일을 'E' 드라이브의 USB에 저장을 시도하였으나 접근할 수 없음을 알리는 메시지가 표시되고 작업이 종료되었다. 제어가 설정된 외장형 HDD에 파일의 저장을 시도하였지만 결과는 동일하여 설정된 제어 기능이 정상적으로 수행되었다.



(그림 12) Access Deny로 제어를 설정하는 화면



(그림 13) Access Deny로 설정된 USB에 파일 저장

컴퓨터 B에서 FDD, HDD, 외장형 HDD, USB에 'Read Only'와 'Access Deny'로 설정하고 총 30회 제어가 수행되는지를 확인하였고 그 결과는 <표 4>와 같다.

〈표 4〉 저장장치의 제어 수행 횟수

운영체제	제어 형태	시험횟수	제어 수행 횟수				
			FDD	가상드라이브	외장형 HDD	USB	네트워크 공유
Windows XP Pro	Read Only	30회	6회	6회	6회	6회	6회
	Access Deny	30회	6회	6회	6회	6회	6회
Windows 2000	Read Only	30회	6회	6회	6회	6회	6회
	Access Deny	30회	6회	6회	6회	6회	6회

이와 같이 드라이브나 디바이스로 인식된 저장장치에 파일의 저장이나 접근을 시도하는 경우에 설정된 제어가 정확히 수행되어 설계된 기법이 적정하게 수행됨을 확인하였다.

5. 결론 및 향후과제

본 연구를 통하여 서버에서 클라이언트의 드라이브나 디바이스로 제어를 설정한 후 사용자가 제어가 설정된 장치에 파일의 저장을 시도하면 수행할 수 없도록 제한하여 파일의 생성자도 관리자의 허락이 없이는 파일을 복사하거나 저장할 수 없어 유출을 방지할 수 있는 방법을 연구하고 시스템을 구현하였다. 이러한 방법으로 클라이언트에 저장된 파일의 유출을 방지할 수 있도록 서버에서 제어로 회사 내의 중요한 파일이나 도면 등의 자료를 클라이언트에서 관리가 가능하여 내부보안을 크게 강화 할 수 있게 되었다. 네트워크 공유에서 제어를 설정하면 해당 클라이언트에 저장된 파일에 대한 접근을 제한 할 수 있는 방법과 시리얼 통신을 이용한 저장장치에 대한 유출방지 방법에 대해서는 추가 연구가 필요하다. 또한 파일의 유출경로에는 인터넷 통신을 이용하는 e-mail이나 web mail, web hard와 Messenger를 통하여 유출하는 경우와 무선랜, Bluetooth통신, 적외선 통신 등으로 전송하는 방법이 있어 클라이언트내에 저장된 파일의 유출을 방지하기 위해서는 저장장치 외에 통신방법에 대한 연구가 요구된다.

참 고 문 헌

[1] 최현희, 정태명, "통합보안관리시스템을 위한 보안정책 일반화에 관한 연구", 정보처리학회 논문지C, 제9-C권, 제6호, pp. 823-824, 2002.

[2] 김진성, 안병혁, "보안 기법을 적용한 전자문서 관리 모듈의 설계", 산업경제, 제12집, pp. 31-46, 2001.

[3] 박승기, "Windows 2000 서버 보안의 관한 연구", 석사학위본문, 동국대, pp. 26-32, 2002.

[4] 박정삼, "NT서버 실시간 이벤트 감시시스템의 설계 및 구현", 석사학위본문, 대전대, 2003.

[5] 이남훈, "Windows 2000기반의 파일보호 시스템 설계 및 구현", 석사학위논문, 홍익대, 2000.

[6] 김대중, "커널 모듈을 이용한 접근제어 설계 및 구현", 석사학위논문, 한서대, 2002.

[7] 신영선, "Windows 2000기반 파일접근 감시시스템의 설계 및 구현", 석사학위논문, 대전대, 2004.

[8] 이상수, 김영수, 한종욱, 정교일, 손승원, "보안프로세서의 동향 및 성능 비교", 정보보호학회지, 제13권, 제4호, pp. 15-18, 2003.

[9] 주학수, 김승주, "암호화 제품의 개발현황", 정보보호학회지, 제12권, 제5호, p. 2, 2002.

[10] 김삼용, "Windows 운영체제에서 파일시스템 보호", 석사학위논문, 항공대, pp. 15-19, 2001.

[11] 김종원, 최종욱, "기업 정보 유출 방지를 위한 기술", 정보처리학회지, 제10권, 제2호, p. 88, 2003.

[12] 최진선, "내부 중요 정보 유출 차단 시스템 구축에 관한 연구", 석사학위논문, 한양대, pp. 25-27, 2004.

[13] 주학수, 김대엽, 장기식, 김승주, "디지탈 저작권 관리 시스템(DRM)의 개발현황", 정보보호학회지, 제13권, 제2호, p. 82, 2003.

[14] 차성철, "KMS기반에서의 DRM을 이용한 문서보안 시스템 구현에 관한 연구", 석사학위논문, 성균관대.

최 주 호

1978년 한양대학교 산업공학과 졸업
1994년 숭실대학교 정보과학대학원 석사
2006년 숭실대학교 대학원 컴퓨터학과(공학박사)
1997년 정보처리기술사(정보관리 분야), 정보시스템 공인감리인
2002년~현재 (주) 디지탈센스
1987년~2002년 벽산정보산업(주), (주)에스원
관심분야 : 컴퓨터/네트워크 보안, 산업보안, 정보시스템 감리

류 성 열

1997년 아주대학교 컴퓨터학부 (공학박사)
1997년~1998년 George Mason University 교환교수
1981년~현재 숭실대학교 정보과학대학 컴퓨터학부 교수
1998년~2001년 숭실대학교 정보과학대학원 원장
1998년~2005년 숭실대학교 전자계산원 원장
관심분야 : 소프트웨어 유지보수/재사용, 소프트웨어 재공학/역공학, 정보보호 등