

## 원도우 기반 파일 감시시스템의 설계 및 구현

\*신영선, \*박진섭, \*이지영, \*\*오송석, \*\*\*김황래  
대전대학교 컴퓨터공학과

### Design and Implementation of File Monitoring System based on Windows

\*Young-Sun Shin, \*Jin-Sub Park, \*Ji-Young Lee, \*\*Song-Suk Oh, \*\*\*Hwang-Rae Kim  
\*Dept. of Computer Engineering, Daejeon University  
\*\*Dept. of Liberal Arts, Konyang University  
\*\*\*Dept. of Computer Engineering, Cheonan National Technical Colleage

#### 요약

정보시스템의 활용도가 높아지면서 네트워크를 통해 보다 빠르게 상호간 정보체계를 공유하게 됨으로써 컴퓨터 통신망을 통해 내부정보의 위치 또는 변조, 유출되는 등 각종 불법 행위가 급증하고 있다. 이에 본 논문에서는 내부 정보보안 사고에 대한 적극적인 보안수단을 제공하기 위해 내부사용자에 의한 파일유출을 감시하고 중요파일에 대한 접근시도 및 접근동작에 대해 로그정보를 분석하여 보안사고 발생시 입증할 수 있는 근거를 제시하고자 파일 감사시스템을 설계하고 구현하였다.

#### 1. 서론

네트워크를 통한 정보공유에 따라 기업 및 개인까지도 보다 빠르게 상호간 정보체계를 공유하게 되었다. 그러나 이러한 네트워크 환경으로 인해 악의적인 해킹, 사이버 범죄 등의 역기능 현상도 증가하면서 컴퓨터 통신망을 통해서 개인용 컴퓨터의 정보가 위조 또는 변조되고, 허락없이 유출되는 등 각종 불법 행위가 급증하게 되었다.

이러한 위험을 사전에 방지하기 위하여 네트워크 보안대책 방안으로 침입차단시스템(Firewall), 침입탐지시스템(IDS), 가상 사설망(VPN) 등과 같은 보안 제품들을 설치, 운영하고 있다. 하지만 이러한 보안제품들의 한계성으로 인해 안전성이 확보되지 못하고 있다. 이에 여러 PC보안 제품들이 개발되었으나 이러한 제품들은 외부 사용자의 접근에 대해 실시간으로 탐지하고 즉각적인 대응에 초점을 두고 개발되었기 때문에 전체 보안사고 중 80% 이상을 차지하는 내부 정보보안 사고(내부정보유출 및 정보자원 남용)에 대한 적극적인 보안수단이 필요한 실정이다.

또한 침입이나 불법적인 접근이 이루어진 후에 수많은 시스템 로그에 대한 분석 및 보호가 이루어지지 않

아 중요 파일 유출시 입증할 수 있는 근거 자료제시가 미비한 상태이다. 따라서 보안 제품의 한계성에 대한 차선책으로 외부사용자뿐 아니라 내부사용자로 인해 중요파일이 유출되었을 경우 접근 감시와 시스템로그에 대한 효율적인 관리를 통해 중요파일유출시 입증할 수 있는 기술이 필요하다.

본 논문에서는 내부사용자에 의한 파일유출을 감시하고 중요파일에 대한 접근시도 및 접근동작, 침입발생시 효과적인 대응을 수행할 수 있도록 한다. 또한 각 모듈별 로그 분석과 관리를 통하여 보안사고 발생시 입증할 수 있는 근거 자료를 제시하고자 하는 것이 본 논문의 목적이다. 본 논문의 구성은 다음과 같다. 제1장 서론에 이어 2장에서는 파일 감사시스템을 설계하고, 제3장에서 이를 구현한다. 마지막으로 결론 및 향후 연구방향을 제시하고자 한다.

#### 2. 관련연구

##### 2.1 공유폴더 취약점 연구

공유폴더는 응용프로그램, 데이터라고 불리는 각 사용자별 데이터등을 네트워크상에서 공유하는 것으로

불법 접근으로 인한 여러 가지 취약점들이 나타나고 있다. 임의의 사용자가 해킹툴이 아닌 NetBIOS over TCP/IP 기능을 이용하여 포트 137, 138, 139번을 통해 원격 PC의 공유된 디스크나 폴더로 접근하여 파일을 복사하거나 지우는 해킹행위를 할 수 있다. 또한 Windows 2000/XP에서는 TCP포트 445상에서 TCP/IP를 통해 직접 SMB의 기능을 이용하여 부적절한 패킷 요청을 전송함으로써, 서버기기에 서비스 일부 공격을 일으키고 이를 통해 시스템을 중단시킬 수 있다. 국내에서는 공유풀더에 대한 취약점에 대응하기 위해 CERTCC에서 공유풀더 취약점을 이용한 공격 유형에 대해 취약점 대응 방법을 제시하였다[11].

공유풀더 취약점으로 인해 웜·바이러스가 유포되거나 자신의 시스템이 다른 사용자에게 노출되어 개인 정보가 유출 당할 수 있으며 취약점을 통해 원격에서 조정 당할 수 있으므로 시스템 점검이 필수적이어야 한다. [표 1]은 수많은 웜·바이러스가 중에 목적이 공유풀더 취약점을 이용한 공격을 나타내는 표이다.

[표 1] 공유풀더 취약점을 이용한 웜·바이러스

바이러스명	특징
Delorder	- 네트워크 공유를 통해 전파된다. - 바이러스에 감염되면 445포트를 스캔하여 administrator 계정으로 접속을 시도한다.
LOVEGATE	- 메일 및 암호가 취약한 관리목적 공유풀더로 전파된다. - 20168 포트가 오픈된다.
Opaserv	- 네트워크 환경에서 C드라이브가 읽기/쓰기가 공유된 시스템 - 137번트(NetBIOS Name Service)을 사용하여 동일 네트워크와 인접한 네트워크를 랜덤하게 검색한다.
FunLove	- 특별한 파괴동작은 없으나 시스템이 느려진다. - 네트워크를 통하여 감염되기 때문에 감염 속도가 매우 빠르다.
Netspree	- 윈도우 2000의 IPC\$공유된 시스템들을 대상으로 전파, 설치된다. - 연결대상은 윈도우 2000에 기본 ipc\$를 이용한다.

## 2.2 관련기술 동향

현재 PC보안 제품들은 외부의 불법적 접근을 중심으로 정보의 무단 유출과 해킹등의 위협으로부터 시스템을 보호하는 목적으로 개발되어 내부 사용자에 대한 보안대책이 미흡한 설정이다. 또한 중요파일에 대한 예방과 감시에만 목적을 두고 있어 중요파일 유

출시 내부사용자에 대한 파일 유출 감사 목적의 대상이 되고 있지 않은 상태이다. 다음은 현재 PC보안 제품들이 사용하는 기술로 중요파일의 외부 유출과 위·변조를 예방하고 보안성 있게 정보를 전달하기 위한 다음과 같은 특징을 갖는다.

- 모니터링 기술
- 침입차단기술
- 파일 암복호 기술
- 로그관리기능
- 공유풀더 접근 통제 기능

## 2.3 파일 감사시스템 요구사항

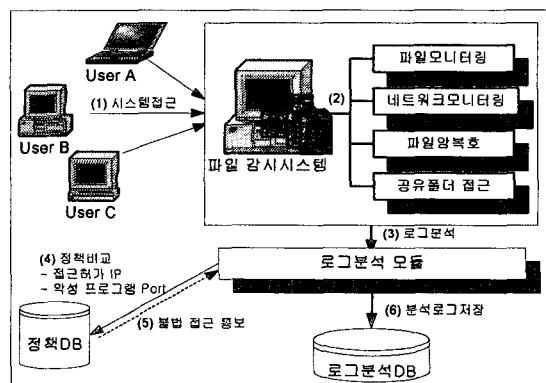
본 논문에서 제시하는 시스템의 요구사항은 다음과 같다.

- 실시간으로 모든 접근에 대해 모니터링
- 시스템 관리자만이 정책 설정
- 인증된 사용자만이 저장된 로그정보에 대한 접근 할 수 있도록 제한
- 인증된 사용자만이 파일에 대한 감시와 파일 암호화 및 제어
- 모든 로그정보의 저장 뿐 아니라 로그에 대한 분석과 통계를 통해 파일 유출 시 접근 사용자에 대한 감사정보를 제공

## 3. 파일 감사시스템 설계

### 3.1. 시스템 구조

파일 감사시스템의 전체구조는 파일 모니터링 모듈, 네트워크 모니터링 모듈, 파일 암복호 모듈, 공유풀더 접근제어 모듈과 각 모듈에서 생성된 로그 정보를 통해 파일 유출시 입증하기 위해 효율적으로 분석하고 관리하는 모듈로 구성된다. (그림 1)은 파일 감사시스템의 전체 구조를 보여준다.



(그림 1) 파일 감사시스템의 전체 구조

### 3.2 각 모듈별 설계

#### (가) 파일 모니터링 모듈

시스템내의 중요파일을 보호하고자 하는 것으로 특정 디렉토리, 특정 파일에 대한 접근 시도 및 접근 동작에 대해 실시간으로 모니터링 한다. 정책 데이터베이스에 저장되어 있는 불법사용자의 IP주소나 악성포트로의 접근일 경우 정상적인 사용자와 다르게 구분하여 나타내었다[7-9]. 이러한 모든 접근을 데이터베이스에 저장하고 불법사용자가 파일에 접근하여 파일을 삭제하거나 변조, 유출시 정책을 설정하여 비교함으로써 파일 접근에 대한 접근을 감시한다[12].

#### (나) 파일 암복호 모듈

파일 유출시 파일을 보호하기 위한 목적으로 128비트 암호 알고리즘을 사용(3DES, AES, SEED)하여 한 가지 알고리즘이 아닌 다양한 알고리즘을 사용자가 선택하여 파일에 대한 암복호를 수행할 수 있도록 한다. 또한 파일에 대한 암복호 동작과 접근 시간, 사용자등의 정보를 저장하여 관리한다[3][5].

#### (다) 공유폴더 제어 모듈

네트워크 드라이브를 통해 접근하는 사용자로부터 파일을 보호하기 위한 것으로 공유폴더에 대한 접근 및 동작에 대해 모니터링 함으로써 불법접근에 대하여 실시간으로 사용자에게 알려주고 모든 공유폴더 접근에 대한 로그데이터를 생성하여 저장한다[1-2].

#### (라) 정책설정 모듈

시스템에 해를 가할 수 있는 기능(허가 받지 않은 IP, 악성프로그램 Port)들을 정책 데이터베이스에 저장하여 접근에 대해 미리 제한할 수 있도록 정책을 설정한다.

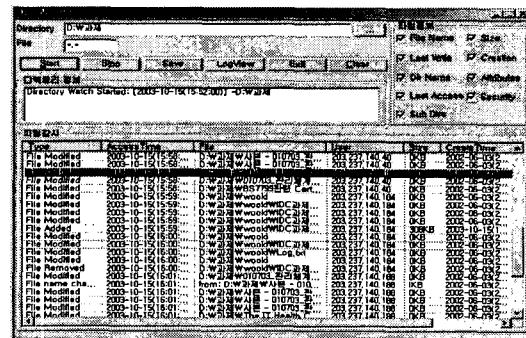
#### (마) 로그분석모듈

각 모듈별로 저장된 로그데이터들을 분석하여 파일에 접근하는 모든 정보를 사용자에게 제공하도록 한다. 프로토콜별, 포트별, 일별, 월별 등의 검색기능과 통계 기능을 제공하여 사용자가 편리하고 정확하게 로그 데이터를 분석하여 불법 침입과 접근에 대한 정보를 쉽게 파악하여 대응할 수 있도록 한다.

### 4. 파일 감시시스템의 구현

본 절에서는 위의 파일 감사시스템의 설계를 구현하였다. (그림 2)는 파일 모니터링 화면으로 특정 디

렉토리를 지정하여 디렉토리 안에 있는 파일에 접근하는 경우 실시간으로 모니터링 하여 접근 정보를 나타내게 된다. 접근정보로는 파일에 대한 동작, 접근시간, 파일명, 접근한 사용자 IP, 파일 크기 등이다.



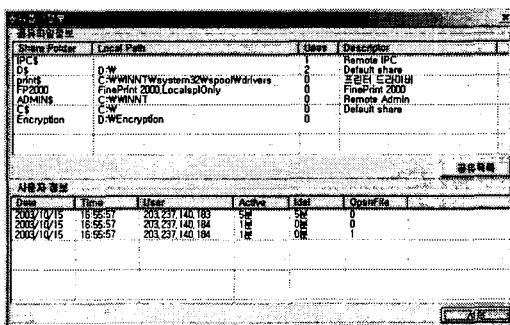
(그림 2) 파일 모니터링 화면

(그림 3)은 파일 모니터링 로그정보를 나타낸다. 파일에 대해 모니터링한 모든 정보를 저장하고 파일명, 접근 시간등의 검색기능을 제공하여 관리자가 파일에 대한 접근 정보를 쉽게 관리하고 파일 유출시 입증할 수 있는 근거자료를 제시하도록 한다.

FileMode	FileAccess	FileName	FileSize	AccessTime	CreateTime
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Added	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Removed	D:\WDA\wood	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Removed	D:\WDA\IT Health	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File name change	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-
File Modified	D:\WDA\WDA - The IT Health Check Service (2).doc	[0KB]	[203,237,40,19]	2013-10-15 16:	2012-07-

(그림 3) 파일 모니터링 로그정보

(그림 4)은 공유폴더 접근에 대한 정보를 실시간으로 나타내는 화면이다. 네트워크 드라이브를 통해 공유폴더에 접근하는 사용자에 대해 실시간으로 공유폴더에 접근한 사용자 정보, 접근시간, Active 시간과, Idle 시간, 열린 파일 수 등의 정보를 얻을 수 있고, 이러한 모든 정보를 데이터베이스에 저장하도록 하였다.



(그림 4) 공유폴더 접근제어 실행화면

(그림 5)은 공유폴더에 접근한 정보를 데이터베이스에 저장하여 공유폴더 접근 로그를 보여주는 화면이다. 접근 시간과 접근 사용자 IP주소, 열린 파일수에 대한 정보를 나타낸다. 또한 불법적인 접근에 대해서는 정상적인 접근과 다르게 표시하고 날짜별, 접근IP별로 검색할 수 있도록 하여 관리자가 쉽게 공유폴더에 대한 불법 접근을 확인할 수 있도록 하였다.

No	Date	Time	User	OpenFile
1	2003/10/15	16:54:31	203.237.140.184	0
2	2003/10/15	16:54:35	203.237.140.183	0
3	2003/10/15	16:54:37	203.237.140.183	0
4	2003/10/15	16:54:42	203.237.140.184	0
5	2003/10/15	16:54:42	203.237.140.184	0
6	2003/10/15	16:54:45	203.237.140.184	0
7	2003/10/15	16:54:45	203.237.140.183	0
8	2003/10/15	16:54:45	203.237.140.183	0
9	2003/10/15	16:54:45	203.237.140.183	0
10	2003/10/15	16:55:43	203.237.140.184	0
11	2003/10/15	16:55:43	203.237.140.184	0
12	2003/10/15	16:55:43	203.237.140.184	0
13	2003/10/15	16:55:43	203.237.140.183	0
14	2003/10/15	16:55:43	203.237.140.183	0
15	2003/10/15	16:55:43	203.237.140.183	0
16	2003/10/15	16:55:43	203.237.140.184	0
17	2003/10/15	16:55:43	203.237.140.184	0
18	2003/10/15	16:55:43	203.237.140.184	0
19	2003/10/15	16:55:43	203.237.140.184	0
20	2003/10/15	16:55:57	203.237.140.183	0
21	2003/10/15	16:55:57	203.237.140.184	0
22	2003/10/15	16:55:57	203.237.140.184	0
23	2003/10/15	16:55:57	203.237.140.184	0
24	2003/10/15	16:57:39	203.237.140.183	0
25	2003/10/15	16:57:39	203.237.140.184	0
26	2003/10/15	16:57:39	203.237.140.184	0
27	2003/10/15	16:57:39	203.237.140.184	0
28	2003/10/15	16:57:39	203.237.140.184	0
29	2003/10/15	16:57:39	203.237.140.184	0
30	2003/10/15	16:57:39	203.237.140.184	0

(그림 5) 공유폴더 접근로그

## 5. 결론

본 논문에서는 내부 사용자를 대상으로 하여 중요파일에 대한 접근 및 유출을 감시함으로써 내부 중요파일 유출시 입증할 수 있는 근거로 활용하기 위하여 파일 감시시스템을 설계 및 구현하였다. 본 논문의 결과는 파일 유출시 접근한 사용자에 대해 감사하기 위한 증거자료 제시, 네트워크 접근 사항과 개인 시스템 및 중요 파일에 대한 보호와 내부 사용자에 대한 보안강화를 통해 좀 더 안정적인 환경에서 시스템을 운영

할 수 있도록 하였다.

향후, 서버-에이전트 개념을 도입하여 에이전트에 대한 정보관리를 실시간으로 서버로 전송하여 에이전트의 정보를 보호하고 통합적으로 관리해야 할 것이다. 또한 수많은 로그에 대한 보안대책으로 로그에 대한 무결성을 보장하기 위한 연구도 지속적으로 이루어져 내부 사용자에 대한 감시를 통하여 파일유출시 로그를 분석함으로써 좀 더 안정적인 환경을 제공하는 효과를 가져올 것으로 전망된다.

## [참고문헌]

- [1] RFC 1001 : Protocol standard for a NetBIOS service on a TCP/UDP transport : Concepts and methods, 1987
- [2] RFC 1002 : Protocol standard for a NetBIOS Service On a TCP/UDP Transport : Detailed Specifications, 1987
- [3] 128-Bit Symmetric Block Cipher(SEED), 정보통신 단체표준(TTAS), 1999.9
- [4] Data Encryption Standard(DES), FIPS PUB 46-3, 1999. 10
- [5] Advanced Encryption Standard(AES), FIPS PUB 197, 2001.11
- [6] David. J., "Computer Intrusion Detection and Network Monitoring", Springer, 2001.
- [7] Stephen Northcutt 외 2명, "Intrusion Signatures and Analysis", 2001
- [8] Roberta Bragg, "Windows 2000 Security", 2001
- [9] Charlie kaufman 외 2명, "Network security private communication in a public world", 2002.
- [10] W.Richard Stevens, "TCP/IP Illustrated, Volume1", 1999
- [11] "윈도우즈 환경에서의 공유폴더 취약점을 이용한 공격 유형 및 취약점 대응 방법", CERTCC-KR, 2003.4
- [12] 박영철 외 3명, "멀티유저 윈도우 환경에서의 실시간 데이터 접근 모니터링 시스템 설계 및 구현", 한국멀티미디어학회 2003.