
윈도우 XP 기반의 파일 정책 모듈 설계 및 구현

성 경*

Implementation of File Access Control Module Using on Windows XP

Kyung Sung*

요 약

최근 급속한 정보통신기술의 발달에 따라 네트워크를 통한 정보의 공유와 개방화가 가속화되면서 정보시스템은 다양한 보안 위협에 노출되어 있으며 각종 보안 사고가 사회적 문제로 대두되고 있다. 이에 따라 시스템을 안전하게 보호하기 위하여 조직의 잠재적인 보안위협을 관리하고 시스템에 대한 공격에 대비하기 위하여 침입차단시스템, 침입탐지시스템, 가상 사설망 및 취약점 스캐너 등의 다양한 보안도구 들이 운영되고 있다. 이러한 보안 시스템은 전문가적인 지식이 필요하며 일반 사용자가 운영 하기가 쉽지 않다.

본 논문에서는 공격에 대한 탐지가 아닌 윈도우상에서 리눅스와 유닉스에서와 같이 각각의 파일에 대한 정책을 세워 침입자의 파일에 대한 무결성, 부인 방지를 할 수 있다.

ABSTRACT

As the development of information telecommunication technology and thus the information sharing and opening is accelerated, IT system is exposed to various threatener and the avrious security incident is rasing its head with social problem. As countermeasure, to protect safely and prepare in the attack for a system from a be latent security threat, various security systems are been using such as IDS, Firewall, VPN etc.. But, expertise or expert is required to handle security system. The module, implemented in this paper, is based on Windows XP, like Linux and Unix, and has effect integrity and non-repudiation for a file.

키워드

파일접근 제어 모듈, 파일정책, 보안 운영체제, 마이크로 커널

1. 서 론

최근 급속한 정보통신기술의 발달에 따라 정보 시스템은 과거 인간이 상상하지 못했던 편리함과 신속성을 제공하고 있으며, 시스템에 저장된 정보는 각종 컴퓨터와 네트워크를 통하여 모든 사람에게 서비스됨으로써 누구나 문명의 이기를 공유할 수 있게 되었다.

침해사고를 예방하고 효과적인 대응방법을 마련 하기 위해 침입차단기술, 침입탐지기술 등 여러 가지 정보보호기술들이 개발되어 왔다. 그러나, 이와 같은 기술들은 알려진 취약점에 대한 예방과 탐지에 대해서는 좋은 결과를 보여주지만, 알려지지 않은 취약점이나 공격에 대해서는 적절한 대응이 쉽지 않은 단점이 있다. 또한 대개의 침해사고 피해 발생 시 중요한 서비스를 중단하게 되며, 이 경우

매우 중대한 문제를 야기 시킬 수도 있다. 이와 같이 알려지지 않은 취약점이나 공격에 의한 침해사고 대응방법이 요구된다.

침입탐지 시스템이나 침입차단 시스템이 네트워크를 통한 침입 대응방법이었다면 본 논문에서 제시되는 파일 접근 제어는 시스템에서의 침해에 대한 대응방법이다. 본 논문에서는 윈도우즈 운영체제에서 사용할 수 있는 파일 접근 제어 모듈을 설계 및 구현함으로써 알려지지 않은 새로운 침입 유형에 대해서 파일을 수정 및 삭제시키지 못하게 함으로써 침해에 대응 할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 보안 운영체제에 대하여 알아보고 3장에서는 윈도우즈 기반의 파일 정책에 대해 알아봄 4장에서는 본 논문에서 제시하는 모듈에 대한 설계와 구현에 대하여 서술한다. 마지막으로 4장에서는 결론을 맺는다.

II. 보안 운영체제

2.1 보안 운영체제

보안 운영체제란 기존의 커널에 보안 기능을 통합시킨 보안 커널(Secure Kernel)이 추가로 이식된 운영체제로 참조 모니터(Reference Monitor) 개념을 정의한 TCB(Trusted Computing Base)의 하드웨어, 펌웨어, 소프트웨어의 요소를 뜻한다[1].

보안 운영체제의 기능을 살펴보면 다음과 같다.

- 사용자에 대한 식별 및 인증
- 강제적 접근 통제(MAC : Mandatory Access Control)
- 임의적 접근 통제(DAC :Discretionary Access Control)
- 재사용 방지(Object Reuse Prevention)
- 침입 탐지(Intrusion Detection)

보안 커널[2]의 가장 중요한 부분으로 참조 모니터의 기능을 살펴보면 다음과 같다.

- 객체에 대한 접근 통제 기능을 수행한다.
- 감사, 식별 및 인증, 보안 매개변수 설정 등과 같은 다른 보안 매커니즘과 데이터를 교환하면서 상호 작용한다.

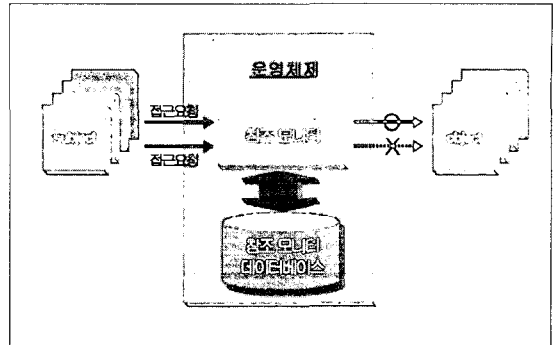


그림 1. 보안 운영체제 개념도
Fig 1. Secure OS conceptual diagram

참조 모니터 구현은 시스템 콜 엔트리(윈도우 NT의 경우 Service Table)에서 원래의 커널의 시스템 콜 주소를 저장한 후, 참조 모니터 함수의 주소를 시스템 콜 엔트리에 저장한다.

보안 커널의 보안 기능을 살펴보면 다음과 같다[3].

- 식별 및 인증 : 고유한 사용자 신분에 대한 인증 및 검증
- 강제적 접근 통제 : 사용자의 접근결정에 대해 고정된 보안 속성을 보안 관리자 또는 운영체제에 의해 정해진 엄격한 규칙에 따라 자동적으로 부여함으로써 사용자의 자유 재량에 상관없이 강제적으로 접근 통제
- 임의적 접근 통제 : 사전에 보안 정책이나 보안 관리자에 의해 개별 사용자에게 합법적으로 부여한 한도 내의 재량권에 따라 사용자가 그 재량권을 적용해 접근 통제
- 객체 재사용 방지 : 메모리에 이전 사용자가 사용하던 정보가 남아 있지 않도록 기억장치의 공간을 깨끗이 정리
- 완전한 중재 및 조정 : 모든 접근 경로에 대한 완전한 통제
- 감사 및 감사 기록 축소 : 보안 관련사건 기록의 유지 및 감사 기록의 보호, 막대한 양의 감사 기록에 대한 분석 및 축소
- 완전한 경로 : 패스워드 설정 및 접근 허용의 변경 등과 같은 보안 관련 작업을 수행할 때 안전한 경로 제공
- 침입 탐지 : 정상적인 시스템의 사용 패턴을 분석하고, 비정상적인 사용이 발생했을 때 이에 대한 경보 제공

보안 커널의 구현 방법은 커널을 새로이 구현하

는 방법과 모듈방식으로 만들어 모듈을 커널 속에 심는 방법(LKM: Loadable Kernel Module)등 두 가지 방법이 있으며, 통합 커널 기반 방식은 기존 운영체제의 모든 기능을 포함하고 API는 커널 서비스를 이용하게 하며, 마이크로 커널 방식은 이와 대조적으로 기존 통합 커널을 최소화하고 시스템을 최대한 모듈화 한다.

마이크로 커널이란 범용 운영체제로 사용될 것을 염두에 둔 운영체제로써 커널의 조립성을 확장성이라는 면에 초점을 두고 연구, 개발되어 왔다. 특히 상업용 시스템의 경우 전통적으로 동적으로 적재 가능한 확장 모듈, 예를 들면 디바이스 드라이버, 설계 당시에는 고려하지 않았던 새로운 서브시스템(subsystem), 새로운 파일 시스템 등을 지원할 수 있는 경로, 즉 인터페이스를 제공하는 방식을 택해왔다. 이것은 일종의 일체형 커널 모델로서 매우 현실적인 접근 방식이기는 하지만, 커널의 안정성(reliability)에 대해서는 특별한 대책이 없는 것이 또한 현실이다. 이에 확장성에 대한 기존의 방식과는 전혀 다른 새로운 모델이 제시되었는데 이것이 마이크로 커널 모델이다. 운영체제가 지원해야 하는 커널의 기능이 하나의 커다란 커널에 모아져 있던 일체형 커널과 달리, 마이크로 커널은 커널을 최소화하고 커널 외부에 필요한 기능을 제공하는 서버를 구현하는 접근 방법을 택하고 있어, 기본적으로 커널은 주소 공간(address space) 관리, 프로세스간 통신(IPC), 그리고 기본적인 스케줄링 기능만을 제공한다는 것이다. 디바이스 드라이버를 포함한 모든 기능들은 서버형태로 사용자 모드에서 수행하면서 커널 입장에서 다른 사용자 응용 프로그램과 완전히 동일하게 취급된다. 또한 각 서버들은 자신만의 주소 공간을 갖고 있기 때문에 각 서버에 의해 지원되는 시스템 요소들은 상호간의 간섭으로부터 보호될 수 있게 된다. 이와 같이 마이크로 커널의 경우 1980년 후반에 도입된 이후 폭넓은 범위에서의 유연성과 확장성 지원 등 많은 장점으로 매우 각광을 받았으나, 서버의 기능을 이용하기 위한 빈번한 IPC에 의한 오버헤드와 구현상의 불합리성으로 매우 낮은 성능을 보여 왔다. 따라서 새로운 방향에서 마이크로 커널을 접근하려는 시도되고 있다.

보안 커널은 운영체제 기술 발전의 흐름에 따라 보안 운영체제 또한 기존의 IK(Integrated Kernel: 통합 커널) 방식보다는 MK(Micro Kernel) 방식으로 개발 경향이 변하고 있다.

TCSEC(Trusted computer security evaluation criteria)은 미국 국립 컴퓨터 보안 센터(NCSC)가 1985년 발간한 안전한 컴퓨터 시스템을 위한 평가

지침서로서 컴퓨터 시스템의 보안을 효과적으로 평가하기 위해 6개의 기본 요구 사항을 정의하였으며, 그 사항을 만족시키는 수준에 따라 7가지의 평가 등급을 제시하였다[4].

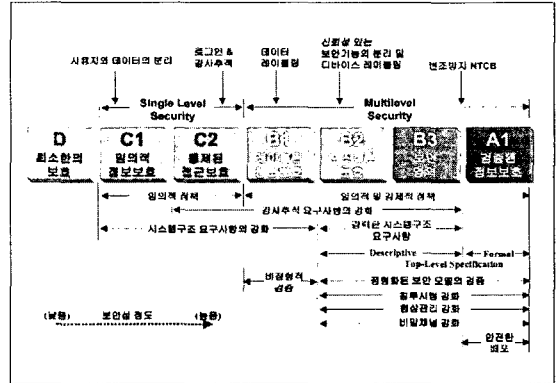


그림 2. TCSEC 평가 기준
Fig 2. Evaluation level of TCSEC

III. 윈도우즈 기반의 파일 정책

3.1 윈도우즈 기반의 보안 모델

윈도우즈 운영 체제하(윈도우즈 NT 이상)에서 지원하는 보안 모델은 유닉스와 마찬가지로 미국 방성이 요구하는 C2 레벨까지 지원하는데 C2 레벨은 다음과 같이 정의 되어 있다.

- 시스템의 자원을 사용자별로 허가하거나 거부할 수 있어야 한다. 예를 들어 같은 팀에 속한 사람들은 파일을 읽을 수 있도록 해야 하되 네트워크를 통해 접속한 다른 사람들은 이 자원에 접근 할 수 없어야 한다. 윈도우즈 운영 체제는 사용자별로 권한을 부여함으로써 모든 자원의 액세스 가능 여부를 통제 할 수 있다.
- 프로세스가 해제한 메모리의 내용을 읽을 수 없도록 보호해야한다. Win32 환경에서는 프로세스까지 독립된 주소공간을 가지므로 서로간의 메모리는 상호 보호된다. 마찬가지로 지워진 파일의 내용도 읽을 수 없어야 하는데 NTFS 파일 시스템은 이를 완벽하게 지원한다.
- 시스템을 사용하는 사람은 반드시 로그인 과정을 거쳐 자신의 신분을 밝혀야 한다. 윈도우즈 운영체제에서는 로그인을 하지 않으면 아무것도 할 수 없도록 되어 있다.

- ㉔관리자는 보안과 관련된 이벤트를 감사할 수 있다. 즉 누가 어떤 일을 하고 있는지 기록을 남기고 그 기록을 관리자가 볼 수 있어야 한다.
- ㉕운영체제는 스스로 자신의 실행 코드를 보호할 수 있어야 한다. 누군가가 운영체제의 커널 코드를 변경하려고 할 때 이를 거부해야 하며 시스템 파일도 수정하지 못하도록 해야 한다.

3.2 보안 설명자

윈도우즈 운영체제의 보안 체계에 의해 보호되는 오브젝트를 보안 오브젝트라고 한다. 보안 오브젝트는 대부분 커널 오브젝트인데, 이름을 가지는 모든 오브젝트와 프로세스, 스레드 등이 이에 해당한다. 이 중 파일과 디렉토리는 NTFS로 포맷된 디스크에 있을 때만 보안이 적용된다. 대부분이 외부 프로세스나 네트워크 통신과 관련된 오브젝트들이며 이런 오브젝트를 생성하거나 여는 API 함수들은 공통적으로 보안 속성을 인수로 요구한다.

가) 보안 설명자

보안 오브젝트는 보안 설정에 따라 사용자별로 사용권한이 달라진다. 이런 액세스 제어가 오브젝트별로 가능하려면 오브젝트 자체에 보안 설정이 기억되어 있어야 한다. 예를 들어 Admin.txt 파일에는 User1은 읽을 수만 있고, User2는 읽고 쓸 수 있다는 보안 설정정보가 기억되어 있다면 이런 보안 설정 정보를 보안 설명자라고 한다. 보안 설명자는 보안 설정 정보를 기억하는 일종의 구조체이며, 그 상세 내부는 공개가 되지 않고 다음과 같은 정보들로 구성되어 있다.

- ㉔소유자의 SID : 오브젝트를 소유하고 있는 사용자의 SID이다. 소유자는 보안 설명자의 DACL 정보와는 상관없이 오브젝트에 대한 모든 권한을 가진다.
- ㉕소유자의 그룹 SID : 소유자가 속한 그룹의 ID이되, 이 정보는 타 운영체제와의 호환성을 위해 존재하며 윈도우즈 환경에서는 큰 의미가 없다.
- ㉖DACL : 사용자별 권한 정보의 목록이다. 누가 이 오브젝트를 읽을 수 있는지 또는 쓰기가 거부되는지 등의 정보들을 기억하고 있다. 보안 설명자의 가장 핵심이 되는 중요한 정보이다.
- ㉗SACL : 오브젝트를 액세스할 때 기록할 감사 정보를 기억한다. 누가 이 오브젝트에 대해 어떤 동작을 할 때 이벤트 로그에 기록을 남기도록 하는 정보가 들어있다.

나) SID

정확한 보안 설정을 위해서는 로그인하는 모든 사용자를 구분할 수 있는 고유한 값이 필요하다. SID(Security Identifiers)는 보안 식별자라고 하며 로그인하는 사용자나 그룹 등에 붙여주는 ID이다. SID는 앞에서 살펴본 보안 설명자에서도 사용되며 보안 설명자 내의 ACE와 액세스 토큰 등에서도 사용된다. SID는 버전, 도메인 정보, 사용자 정보 등을 포함하고 있으며 이진 포맷으로 되어 있다. Win32 API는 SID를 표현하거나 전달하기 위해 문자열로 바꾸어 주는 함수를 제공하는데 SID를 문자열 포맷으로 변경하면 S-1-5-111-222와 같은 모양을 가진다.

다) 액세스 토큰

보안 오브젝트가 허용되지 않은 사용자로부터 보호되기 위해서는 액세스하고자 하는 사람의 신분에 대한 정보와 보안 설명자를 비교해야 할 필요가 있다. 여기서 사용자의 신분에 대한 정보를 액세스 토큰(Access Token)이라고 하며, 보안 설명자와 함께 윈도우즈 운영체제의 보안 체계를 구성하는 중요한 요소이다.

라) ACL

보안 설명자의 보안 정보는 주로 두 개의 ACL(Access Control List)로 구성되어 있으며 ACL은 개별적인 보안 정보 조각인 ACE(Access Control Entry)의 배열이다. ACE는 하나의 보안 설정을 표현하는데 뒤에서 다룰 것이다.

보안 설명자는 두 개의 ACL를 가지고 있다. 하나는 액세스 권한에 대한 목록인 DACL(Discretionary ACL)이며 나머지 하나는 감사 기록을 통제하는 SACL(System ACL)이다. DACL은 여러개의 ACE로 구성되며 누가 이 오브젝트에 대해 어떤 권한을 가지는지에 대한 정보를 표현한다. 시스템은 보안 오브젝트 액세스 요청이 있을 때 DACL의 정보와 액세스 토큰의 사용자 정보를 비교함으로써 요청한 사용자가 권한이 있는지를 검사한다.

마) ACE

ACL은 ACE의 배열이며 ACE(Access Control Entry)는 ACL의 배열 요소이다. ACL은 ACE를 전혀 가지지 않을 수도 있고 복수개의 ACE를 가질 수도 있다. ACE는 실질적인 보안 정보를 가지는 요소라고 할 수 있으며, 보안 설명자나 ACL은 ACE를 담기 위한 그릇일 뿐이다. 보안 오브젝트의 보안 설정을 알고 싶거나 변경하고 싶다면 ACE를 읽고 편집해야 한다. 세가지 종류의 NT는 세가지

종류의 ACE가 있으며 2000 이상은 여섯 개 종류의 ACE가 있다. 이중 세 가지의 기본적인 ACE는 다음과 같다.

- 허가 ACE : 특정 사용자에게 권한을 주기 위한 ACE이다.
- 거부 ACE : 특정 사용자에게 권한을 금지하기 위한 ACE이다.
- 감사 ACE : 특정 사용자의 특정 액세스에 대한 감사 기록을 남기도록 하기 위한 ACE이다.

바) 액세스 권한

ACE의 정보는 누구에게 어떤 액세스 권한을 허가(또는 금지)할 것인가를 지정한다. 각 보안 오브젝트에 적용되는 액세스 권한은 오브젝트별로 다양하다. 읽기, 쓰기, 삭제 등의 공통적인 액세스 권한이 있고 추가, 속성변경, 이동, 복사, 종료, 질의, 정지, 우선순위 변경, 순회 등등 오브젝트별로 고유한 액세스 권한들도 있다. 이렇게 다양한 액세스 권한의 조합을 표현하기 위해 32비트 정수인 액세스 마스크(Access Mask)가 사용된다. 액세스 마스크의 각 비트는 액세스 권한과 일대일로 대응되므로 액세스 마스크는 액세스 권한들을 멤버로 가지는 비트 필드형의 구조체라 할 수 있다.

액세스 권한은 액세스 권한의 적용방법과 범위에 따라 표준형, 고유형, 일반형 세가지로 구분된다.

표준형은 DELETE, READ_CONTROL, SYNCHRONIZE, WRITE_DAC, WRITE_OWNER 등의 다섯 가지로 구분되며 내용은 다음과 같다.

- DELETE : 오브젝트를 삭제할 수 있는 권한
- READ_CONTROL: 오브젝트의 보안 설명자를 읽을 수 있는 권한
- SYNCHRONIZE : 오브젝트를 동기화 할 수 있는 권한
- WRITE_DAC : 오브젝트의 DACL을 변경할 수 있는 권한
- WRITE_OWNER : 보안 설명자의 소유자 정보를 변경할 수 있는 권한

일반형은 GENERIC_READ, GENERIC_WRITE, GENERIC_EXECUTE, GENERIC_ALL 등으로 나뉘며, 내용은 다음과 같다.

- GENERIC_READ: 읽기 권한
- GENERIC_WRITE: 쓰기 권한
- GENERIC_EXECUTE: 실행 권한
- GENERIC_ALL: 모든 권한

IV. 설계 및 구현

4.1 개발 환경

본 논문에서 구현한 모듈은 윈도우 XP Professional을 기본 운영체제로 사용하였으며, 또한 테스트를 위하여 Administrator와 구별하여 또 다른 계정을 하나 두었다. 프로그램 이름은 ACL(Access Control List)이라 하였다. 개발된 프로그램은 모듈이므로 테스트를 목적으로 콘솔 프로그램으로 하였으며 GUI 환경은 하지 않았다. 개발은 Visual C++ 6.0 을 사용하였다.

4.2 구현

윈도우 환경에서의 파일에 대한 보안 객체를 읽고 쓰는 것은 aclapi를 이용하여 사용하면 된다. NTFS 파일 시스템에서는 파일에 보안 설명자를 두었으며 보안 설명자는 두개의 ACL(Access Control List)로 구성되어 있다. ACL은 개별적인 보안 정보 조각인 ACE(Access Control Entry)의 배열이다.

보안 설명자는 두 개의 ACL을 가지고 있으며 하나는 액세스 권한 목록인 DACL(Discretionary ACL)이며 나머지 하나는 감사 기록 작성을 통제하는 SACL(System ACL)이다. DACL은 여러 개의 ACE로 구성되며 각 ACE는 누가 이 오브젝트에 대한 어떤 권한을 가지는지에 대한 정보를 표현한다.

본 논문에서는 이러한 각각의 파일에 대한 ACE에 대하여 읽고, 쓰고, 수정함으로써 각 파일에 대한 보안 정책을 설정한다.

다음은 ACE에 대한 읽는 함수의 일부분을 보여준다.

```

if(GetSecurityInfo(hFile, SE_FILE_OBJECT, OWNER_SECURITY_INFORMATION |
    DACL_SECURITY_INFORMATION, &pOwner,
    NULL, &pDacl, NULL, (LPVOID*)&pSD) !=
    ERROR_SUCCESS)
    return -1;
CloseHandle(hFile);

//소유자 정보
cbName = 0;
cbDomain = 0;
LookupAccountSid(NULL, pOwner, NULL,
    &cbName, NULL, &cbDomain, &pUse);

Name = (char *)malloc(cbName);
    
```


시지창을 볼 수 있다.
다음은 해당 프로그램이 동작하는 화면이다.

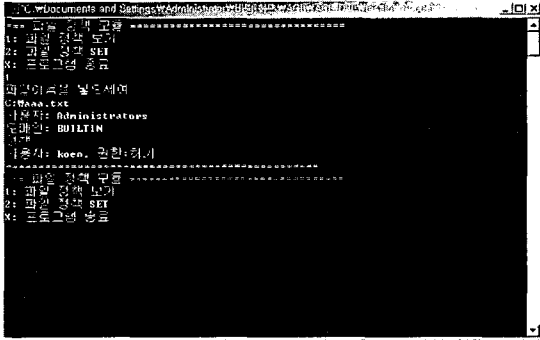


그림 4. ACL 프로그램
Fig 4. ACL program

또한 이 프로그램이 동작하기 위해서는 파일에 대한 등록정보에 파일 정책에 대한 설정을 할 수 없도록 하여야 한다.

윈도즈 환경에서 파일의 등록정보를 보면 다음과 같다.

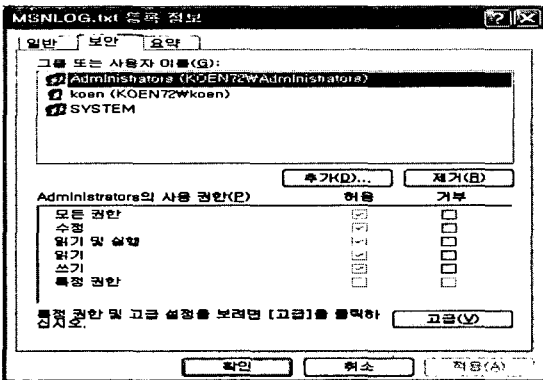


그림 5. 등록정보
Fig 5. Information entity of security

그림 5에서와 같이 등록정보의 보안 탭에서 파일에 대한 정책을 추가, 수정, 삭제 할 수 있다. 본 논문에서 개발된 프로그램은 등록정보에서 보안 탭이 나올 경우 외부 공격자가 보안 정책을 바꿀 수 있기 때문에 보안 탭은 등록정보에 보이지 않아야 한다.

등록정보에서 보안 탭이 나오지 않도록 하려면 레지스트리 키를 변경하면 되는데 레지스트리 키 항목은 다음과 같다.[5]

Hive: HKEY_CURRENT_USER
Key:
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoSecurityTab

위의 값을 변경함으로써 이루어진다. 다음은 레지스트리 키를 변경함으로써 등록정보에서 보안 탭을 보이지 않게 한 그림이다.

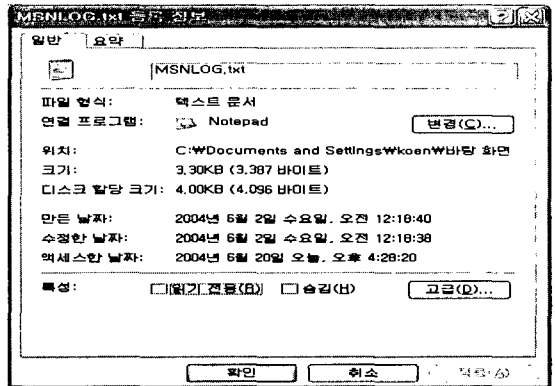


그림 6. 파일 등록정보
Fig 6. Information entity of file

V. 결 론

전 세계가 정보통신의 급속한 발전으로 컴퓨터 및 인터넷의 사용이 급격히 증가함에 따라 정보 처리의 편의성이 증대되는 한편, 컴퓨터 보안에 취약한 일반 사용자들은 정보보호상의 다양한 문제에 처하고 있다. 인터넷을 통한 불법침입으로 시스템의 자원 및 중요한 자료들이 위협 당하고 있고, 때로는 치명적인 손실을 입고 있어 인터넷상에서의 보안 서비스에 대한 필요성이 절실히 요구되는 실정이다[3]. 시스템의 여러 침해사고 중 보안서비스의 미비로 인한 피해가 악의적인 목적으로 인하여 발생한다는 사실을 주지할 때, 이에 대응하여 파일에 대하여 변경 또는 삭제 시 이는 파일정책을 설정함으로써 이러한 시스템 침해사고를 예방할 수 있다.

본 논문에서는 파일 정책 제어 모듈을 설계 및 구현함으로써 윈도우즈XP 기반에서 침해 시 대응할 수 있도록 하였다. 이는 향후 MS계열의 임베디드 OS를 이용한 임베디드 소프트웨어 개발 시 임베디드 시스템을 보호하는 역할을 할 수 있을 것

로 예상된다.

저자소개

참고문헌

- [1] 김재명, 홍기윤, 홍기완, "Secure OS 보안정책 및 메커니즘", 정보보호학회지, 13권 4호, 2003, pp. 49~59
- [2] 이홍섭, 이철원, 이정효, 박정호, "정보통신 기반구조 보호를 위한 보안 커널 개발 동향", 정보보호학회지, 8권 4호, 1998, pp. 63~76
- [3] 소우영 외 3인, "컴퓨터 통신 보안", 그린출판사, 2001, 1월, pp. 603-606
- [4] San Jose, "Common Criteria Solutions", Security Lab, <http://www.fact-index.com/t/tc/tcsec.html>
- [5] <http://is-it-true.org/nt/xp/registry/>

성 경(Kyung Sung)



1998년 8월~1990년 12월 국제
종합기계(주)
1993년 8월 경희대학교 대학원
공학석사
2003년 2월 한남대학교 대학원
공학박사
1994년 3월~2004년 2월 동해대학교 컴퓨터공학
과 교수
2004년 3월~현재 목원대학교 컴퓨터교육과 교수
※관심분야 : 정보관리(정보보호), 신경망, 컴퓨터
교육