PC화일보호시스템에 관한 설계 및 구현

손복만 · 남길현
국 방 대 학 원

Design and Implementation about PC File Security System

Bok Man Son · Kil Hyun Nam
National Defense College

요 약

컴퓨터의 이용이 대중화 되면서 PC의 확대보급으로 데이타 보안의 필요성이 강조되고 있어 본 논문에서는 PC보안의 필요성을 인식하고 PC에서의 처리,운용되는 자료들을 보호하기 위해서 패스워드 인증, 화일속성 변경, DES암호 알고리즘을 이용한 화일암호화 제어, 시스템 액세스 사용자 기록등의 기능을 적용한 PC보안시스템을 설계 및 구현하였다. 특히 키관리에 있어서는 인증을 위한 사용자_ID와 화일 암호화키를 사용자 패스워드로 재암호화시켜 IC카드 대신 플로피 디스켓트에 저장 보관시키고 사용자 패스워드는 사용자 자신이 직접 보관하게 하는 혼용방법을 사용하였다.

I. 서 론

몇년전까지만 해도 대부분의 컴퓨터 연산은 메인프레임 컴퓨터에서 수행되어졌고 데이타 처리 센터에서만 보안의 책임이 있었다. 그리고 시큐리티 개념의 대부분이 복수사용자(multi-user), 공유자원 환경을 가지고 있는 대규모의 메인프레임 시스템에서만 관련되어 있었다. 그러나 최근들어 개인용컴퓨터의 확대보급으로 PC라는 용어가 등장하게 되고 따라서 PC보안이라는 개념도 나타나게 되었다.

PC사용자들은 사용상의 편리함에는 인식을 같이 하지만 PC사용자들 자신에게 직면해 있는 보안의 위험성은 무시해 버리고 또 보안의 대책에 관해서도 생각조차 하지않고 있는 실정이다. 그리고 PC는 전통적으로 공유한다는 생각보다는 단일사용자(Single-user)라는 개념으로써 다루어져 왔기 때문에 PC에 대한 보안은 개인에게 국한

된 사소한 문제로 생각되어 왔다. 그러나 지금은 PC를 자신뿐만 아니라 여러사람이 함께 사용하는 중요한 업무도구로 인식하게 되고 또 대형에서 PC에 이르기까지 시스템 보안에 있어서는 예외가 없게된지 이미 오래이기 때문에 이 보안문제를 거론하는것은 새삼스러운 일이라고 할 수 없다. 그 결과로 정보의 비밀성, 무결성, 가용성에 위협이 존재한다는 인식아래 PC보안이 새롭게 부각되고 있는 것이다.

본 논문에서는 이러한 PC보안의 중요성을 인식하고 효율적이고 사용자에게 편의성을 제공하는 PC화일보호시스템을 모듈화와 시스템 프로그램이 가능한 Turbo-C언어를 사용하여 암호화키를 플로피 디스켓트에 저장 관리함으로써 IC카드를 사용하는 것보다 경제적이 될 수 있고 또 키를 시스템내에 두지않고 디스켓트와 사용자가 분리하여 보관함으로써 안전성도 고려하여 설계 및 구현하였다.

II. 컴퓨터 보안의 개요

컴퓨터 산업의 급속한 발전과 더불어 정보화사회 구현을 위한 컴퓨터 통신의 확장 및 대량의 정보가 컴퓨터를 이용하여 저장, 처리, 전송됨으로써 컴퓨터 보안에 대한 인식이 새롭게 부각되고 있다. 따라서 이러한 컴퓨터 보안의 개념을 정립하고 그에따른 취약성과 보안의 기법에 대해서 살펴보기로 한다.

1. 컴퓨터 보안의 목적

컴퓨터 보안은 컴퓨터와 관련된 하드웨어, 소프트웨어뿐만 아니라 인원 및 시설등에 대해 비인가자의 부당한 행위로 부터 보호함으로써 컴퓨터 시스템의 안전성과 신뢰성 등을 획득, 정보화사회가 가져다주는 편익을 안전하게 누릴 수 있도록 하는데 있다. 따라서 컴퓨터 시스템에 대한 보안은 비밀성, 무결성, 가용성을 유지할 수 있도록 설계 되어야 한다.[2]

첫째, 컴퓨터 시스템은 처리되는 비밀자료들을 암호화하고 시스템 액세스를 제어하여 불법 침입자에게 자료의 비밀성이 노출되지 않도록 하고 반드시 인가된자에 의해서만 액세스가 가능하도록 비밀성(Secrecy or Confidentiality)을 유지하여야 한다.

둘째, 무결성(Integrity) 유지란 단지 인가된자에 의해서만 자료를 변경할 수 있도록 하여 비인가자 및 불법사용자의 자료에 대한 쓰기, 삭제, 생성, 변경등의 액세스로 부터 자료가 보호되어야 하는것을 의미한다.

세째, 가용성(Availability)이란 컴퓨터 시스템을 효율적으로 사용할 수 있도록 거부가 되어서는 안된다는 것을 의미한다. 즉, 정보가 분실되지 않고 항상 획득가능한 상태를 뜻하며 필요시에는 특정시간과 장소에서 즉시 사용할 수 있도록 중복성 유지(redundancy), 데이타의 백업, 물리적 위협요소로 부터의 보호가 이루어져야 한다.

2. 컴퓨터 보안의 취약성

컴퓨터에 대한 보안은 인식이나 관심부족, 부주의, 실수, 태만, 또는 우연한 사고나 의도적인 사고들로 인하여 컴퓨터내의 자료에 대한 취약점을 드러내게 된다. 이에대한 보안위협의 대상은 하드웨어, 소프트웨어, 데이타등으로 분류할 수 있다.[4]

가. 하드웨어 측면에서의 취약성

하드웨어는 겉으로 드러나 있기 때문에 오히려 단순한 보안위협의 대상이 된다. 컴퓨터는 간단한 보호수단이 만들어져 있기는 하지만 컴퓨터는 누수, 화재, 번개, 음식물 부스러기등에 의해서 손상을 입을 수 있다. 그중 가장 심각한 취약점은 컴퓨터실의 의도적인 파괴, 방화, 충격, 또는 컴퓨터 부품의 파괴 및 도난의 행위이다.

특히 최근들어 PC의 보급확산으로 물리적인 보호장치 없이 사무실내에 방치됨으로써 하드웨어적 취약요소가 더해지고 있다.

나. 소프트웨어적 측면에서의 위협

컴퓨터 하드웨어는 소프트웨어(O/S, Utility, 응용 P/G등) 없이는 가치가 없으며 보통 파손의 정도가 겉으로 보여지지만 소프트웨어는 악의적으로 파괴될 수 있고 사고로 변조 및 제거될 수 있어 프로그램상의 변조, 파손등의 행위가 겉으로 나타나지 않으며 더구나 한두개의 코드비트를 수정함으로써 가능하고 결과도 다르게 나타낼 수 있으므로 변조가 매우 쉬운 반면에 탐지는 매우 어렵다는 특성을 갖고 있다. 따라서 소프트웨어 도난 및 불법복사도 소프트웨어적 위협대상에 중요한 부분을 차지하고 있다.

다. 데이타 측면에서의 위협

하드웨어는 컴퓨터 센터의 소수 전문인력에 의해서 보안상 위협이 가해질 수 있고, 소프트웨어는 프로그램을 생성하고 수정하는 인력들에 의해서 가해질 수 있어 커다란 문제가 되고 있다. 데이타 측면에서의 위협도 코드화된 프로그램은 일반인이 인식하기는 어렵지만 리스트된 데이타는 일반인도 쉽게 인식이 가능하여 중요한 자료일 경우에는 그 질과 양에 따라 피해가 커질수도 있다. 따라서 데이타는 그 가치를 상실할때까지는 보호해야 할 필요가 있는 것이다.

3. 컴퓨터 보안의 기법

컴퓨터 보안의 주요대상은 컴퓨터를 중심으로 운영되는 자료들이다. 따라서 이 단원에서는 이러한 컴퓨터내에 저장된 정보를 보호하기 위하여 시스템 인터페이스 보안과 내적보안 측면에서 살펴보고자 한다.

가. 액세스 제어(Access Control) 기법

액세스 제어는 비인가자가 데이타나 프로그램을 우연히 또는 고의로 사용, 추가, 삭제, 변경하는것을 방지하기 위하여 각 사용자에게 화일에 대한 액세스 권한을 명시하여 권한을 가진자만이 액세스를 할 수 있도록 보장하는 것이다. 그런데 이 액세스 제어는 운영체제와 데이타베이스 분야에서 독립적으로 개발되어온 액세스 행렬 모델을 생각할 수 있다. 이 모델은 액세스 제어에 대한 일반적인 보호모델로써 행은 주체(Subject)를 나타내고 열은 객체(Object)를 배열하여 행렬의 원소위치에 액세스 권한(Access rights)을 나타내어 화일이 누구에 의해 어떻게 액세스 될 수 있는가를 정의하는 보호모델이다. 그러나 이 액세스 행렬은 공백이 많은 행렬이므로 효율적이고 공간관리를 위하여 다음 3가지 기법중 한가지에 의해서 구현된다.

각 객체에 대한 액세스 권한을 갖는 모든 주체를 리스트로 정의하는 액세스 리스트(Access List)와 각 주체가 액세스할 수 있는 모든 객체를 리스트로 정의하는 능력리스트(Capability List), 그리고 각 객체는 록크(Lock)를, 각 주체는 키(Key)라는 비트패턴을 가지고 있어 어떤 주체가 액세스 하려고 하는 객체의 록크들 중의 하나와 일치될 경우에만 그 객체를 액세스할 수 있도록 액세스 리스트와 능력 리스트를 절충하여 만든 록크/키(Lock/Key) 기법등이 있다.

나. 정보 흐름 제어(Information Flow Control) 기법

액세스 제어는 객체의 액세스를 통제하지만 주체가 객체안에 있는 정보를 사용하는 것에는 통제를 하지 못하고 있는 실정이다. 따라서 주체는 일단 객체에 액세스가 되면 객체의 정보를 복제하여 누출시킬 수도 있고 정보의 흐름을 불안전한 상태로 만들 수도 있다. 실제로 정보의 누출에 대한 문제점이 많은 것은 액세스 제어의 결함때문이 아니라 정보흐름에 대한 대책이 부족하기 때문이다.[1]

이러한 정보의 흐름제어는 인가권자에 의해 비인가자에게 정보가 유출되는 것을 미리 방지하고 감시하기 위한 것으로 Bell & Lapadula모델과 Lattice모델등이 있다.

(1) Bell & Lapadula 모델

이 모델은 군사적 보안 모델에 적용시키기 위해 개발된 수학적 모델로써 주체가 자기보다 높은 비밀등급의 객체를 판독하는 것을 막고(No read up), 높은 비밀등급의 객체를 읽어 낮은 등급의 객체로 기록하는 것을 방지(No write down)하여 비밀이 높은 등급에서 낮은 등급으로 흐르는 것을 방지하게 한다. 또 이 모델은 다음 두가지 특성을 만족할 때 정보의 흐름이 불안전한 상태로의 전이(transition)를 막아준다.

첫째, SS - property(Simple Security property)
어떤 주체 S가 객체 O에 대한 읽기(read), 실행(execute) 액세스를
하기 위해서는 주체 S가 객체 O보다 비밀수준이 같거나 높아야한다.

둘째, * - property(Star property)

어떤 객체 O에 읽기(read) 액세스가 가능한 주체 S는 특정한 객체 P에 쓰기(write) 액세스를 하기 위해서는 객체 O의 비밀수준이 객체 P의 비밀수준보다 낮거나 같아야 한다.

(2) 래티스 모델(Lattice model)

이 래티스 모델은 Bell & Lapadula 모델에 컴파트먼트 요소를 추가하여 권한수준과 취급범주가 서로 상이한 정보에 대해 최소한의 알아야 할 내용만 제공하는 최소권한의 원칙(Need-to-know)에 의해서 정보의 액세스가 제어되는 것으로써 다음 두가지 조건이 만족할때 주체는 객체에 대한 액세스가 허용된다.

① 주체의 비밀인가는 객체의 비밀수준보다 높거나 같아야 한다.

② 주체는 객체의 컴파트먼트를 포함해야 한다.

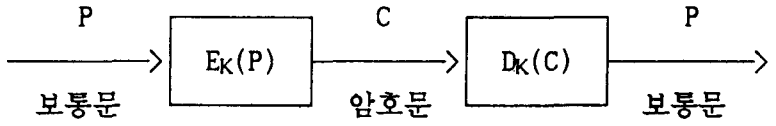
다. 정보 추론제어(Information Inference Control) 기법

이 기법은 불법으로 정보를 얻고자 하는 사람이 개인 또는 집단에 대한 기밀정보를 포함하고 있는 데이타베이스에 여러번의 질문을 통해 획득한 자료로부터 비밀데이타를 추론하지 못하도록 방지하기 위한 기법이다.

이 정보 추론제어 기법에는 데이타베이스에 대한 질문의 양과 질문의 중복을 최소화 시키는 방법, 질문에 응답하기 전에 정확한 답을 흐트려놓는 방법, 그리고 레코드값이 통계계산에 사용되기 전에 무작위로 에러를 삽입하는 방법등이 주로 이용되고 있다.

라. 암호 제어(Cryptographic Control) 기법

암호제어 기법은 [그림 1]과 같이 암호 알고리즘을 이용하여 정보의 형태를 변환시킨후 비밀키를 모르면 어떠한 사용자도 정보내용을 알아볼 수 없도록 하는 기법으로서 컴퓨터 시스템내에 저장된 비밀데이타의 노출에 대한 보호수단이 없는 타 제어기법과 비교가 된다.



P : 보통문(Plaintext)

C : 암호문(Ciphertext)

K : 키(Key)

$E_k(P)$: 키를 이용하여 보통문을 암호화한 암호화 알고리즘

$D_k(C)$: 키를 이용하여 암호문을 복호화한 복호화 알고리즘

[그림 1] 암복호화 시스템

이 암호화에 사용되는 암호 알고리즘은 치환, 재배열, 두가지를 혼합하여 사용하는 혼합방법, 그리고 수학적인 방법등으로 분류된다.

또 여러 암호 알고리즘을 이용하여 실제 시스템에 구현되는 운용방식에는 평문을 연속된 문자나 비트단위로 나누어서 평문길이 만큼의 키 스트림(Key Stream)과 조합하여 암호문을 생성하고 역으로 암호문에서 평문으로 복원시키는 Vernam암호, Running Key 암호와 같은 스트림(Stream) 암호와, 평문 심볼의 집단을 하나의 블럭으로 보고 이 블럭을 기본 단위로써 암호화하는 DES, RSA, Knapsack과 같은블럭(Block) 암호는 메세지 M을 연속적으로 나누어 같은키 K로 암호화 한다.

그중에서도 DES(Data Encryption Standard)는 일반적으로 가장 많이 활용되고 있는 표준화된 암호화 알고리즘이다.

III. PC보안

PC는 주로 가정이나 사무실 환경에서 다루어지고 있는 정보처리 시스템이라고 할 수 있다. 그러나 PC가 확고한 정보처리 시스템으로써 자리를 굳혀가고 있음에도 불구하고 PC보안의 필요성이 크게 인식되지 못하고 있는 실정이다.

본 단원에서는 이러한 PC에 대한 취약성과 그에따른 대책에 관해 고찰해 본다.

1. PC보안의 환경적 취약성

PC는 본질적으로 메인프레임 시스템과 같은 기능을 제공하지만 보안환경이 낮은 PC에서의 취약점들이 존재한다.

첫째, 메인프레임에서의 물리적인 환경보호는 상당한 투자로 비인가자의 시스템 액세스가 어려운 반면에 PC는 개인용이라는 본질적인 개념때문에 상대적으로 접근이 용이하다.

둘째, 대부분의 PC는 중요한 보안에 관련된 시스템 기능들을 사용자가 함부로 액세스 할 수 없도록하는 내장된 하드웨어 메카니즘이 부족하다.

세째, PC는 많은 사람들에 의해서 사용되기 때문에 메인프레임보다 더 중요하고 액세스가 쉬울 수도 있다. 또 PC내의 정보를 손쉽게 액세스할 수 있도록 만들어진 소프트웨어 도구(Tools)들이 많기때문에 데이타에 대한 액세스가 용이하다.

네째, PC의 증가로 인하여 중앙시스템에 대한 의존성이 줄어든 반면에 개인의 책임성이 증가되었으나 PC를 여러사람이 사용함으로써 책임성이 분산되고 사용자들의 전문성 부족으로 보안의 책임성이 부족해졌다.

2. PC보안의 위협요소

PC에 관한 기본적인 시큐리티 문제는 다음 2가지 측면에서 볼때 메인프레임 시스템

보다 더 심각하다.[4]

첫째, PC사용자들은 PC와 관련된 보안의 위험을 잘 이해하지 못한다.
즉, 메인프레임 사용자들에 비해서 경험이나 기술이 부족하다.

둘째, PC 환경하에서는 메인프레임 환경하에서 보다 하드웨어나 소프트웨어 에 대한 보안도구(Tools)들이 적다.

이에따른 PC의 위협요소는 다음과 같이 나타낼 수가 있다.

- PC환경에 대한 위협
- 컴퓨터 고장 및 중요부품의 도난
- 각종 소프트웨어에 대한 결함
- 각종 조작상의 실수
- 해커(Hacker)들에 의한 의도적인 사고

그러나 PC보안의 근본은 PC사용자들의 PC보안에 대한 인식제고도 고려해야 한다.

3. PC보안의 대책

이와같이 PC보안에 관한 취약점들이 많이 나타나고 있지만 다음과 같은 4가지 분야로 집약해서 그에대한 대책을 제시해 보고자 한다.

첫째, 외부침입자의 절도나 물리적인 손상으로부터 PC장비를 보호하는 것이다. 즉 물리적인 시설보안이나 사무실 환경하에서의 화재, 누수, 오염물질 등으로부터 PC와 자기매체에 손상이 가지 않도록 주의를 한다.

둘째, 컴퓨터를 유지하기 위한 궁극적인 목적은 장비보다는 정보를 분석, 처리, 저장하는 능력에 더 가치를 두고있기 때문에 시스템과 데이타에 대한 액세스를 제어할 수 있는 인증이나 논리적인 액세스제어, 화일암호화 기법등을 사용하도록 한다.

세째, 소프트웨어와 데이타에 대한 무결성을 유지하기 위하여 표준화된 개발도구와 대책이 마련되어야 한다.

네째, PC하에서 발생할 수 있는 잠재적인 사고에 대비하여 중요한 자료를 백업시키고 우발적인 사고에 대비한 비상계획을 세워두는 것이 바람직하다.

IV. PC화일보호시스템 설계 및 구현

1. 요구특성

PC보안시스템은 물리적인 환경과 시스템 자체의 보호수단이 필요하지만 보안의 요구수준이 높을수록 PC에 대한 가용성은 반비례한다는 이율배반적인 특성을 고려하여 컴퓨터 보안에 적절한 수준으로 절충하는 것이 바람직하다.

이에대한 고려할 사항은 다음과 같다.

① 데이타 화일에 대한 비밀성을 최대한 유지시킨다.

② 비인가자가 시스템과 데이타를 액세스할 수 없도록 제어시킨다.

③ 사용자는 보안기능이 많을수록 혼돈과 불편함때문에 사용을 기피하게 되고 보안의식이 낮아지게 됨으로 사용자에게 편의성을 제공하도록 하여야 한다.

④ PC의 정보 분실이나 노출은 막대한 결과를 초래할 수 있으므로 중요한 자료에 대한 백업이나 중복자료를 유지함으로써 컴퓨터의 신뢰성을 향상시켜 시스템의 가용성을 높여주도록 하여야 한다.

2. PC보안 기능

PC용 보안장치들은 디스크내의 각종정보를 보호해 주는데 있어서 여러가지 기능들을 제공해 주는데 여기서는 가장 기본적인 사항들만 제시해 본다.

① 시스템 액세스제어. 특정패스워드에 의한 인증이나 중요한 화일에 대한 속성을 변경함으로써 삭제 및 변조를 하지 못하도록 한다.

② 데이타 암호화. 패스워드 제어는 보편적이기는 하지만 일단 노출이 되면 모든 데이타가 노출이 되므로 중요한 화일을 암호화시켜 보관해 두도록 한다.

③ 감사추적. 외부로부터 액세스를 시도하거나 시스템 사용의 흔적이 있는가를 확인하여 불의의 데이타 사고를 미연에 방지할 수 있도록 한다.

④ 부팅방지. PC는 디스크와 관계없이 플로피 디스켓트를 통하여 부팅이 가능하므로 사용자와 도스사이에 약속된 부팅드라이브 외에는 부팅이 불가능 하도록 한다.

⑤ 화일복사 방지. 사용자로 하여금 디스크내의 화일들을 함부로 복사하여 외부에 유출시킬 수 없도록 프로텍트 방법을 사용한다.

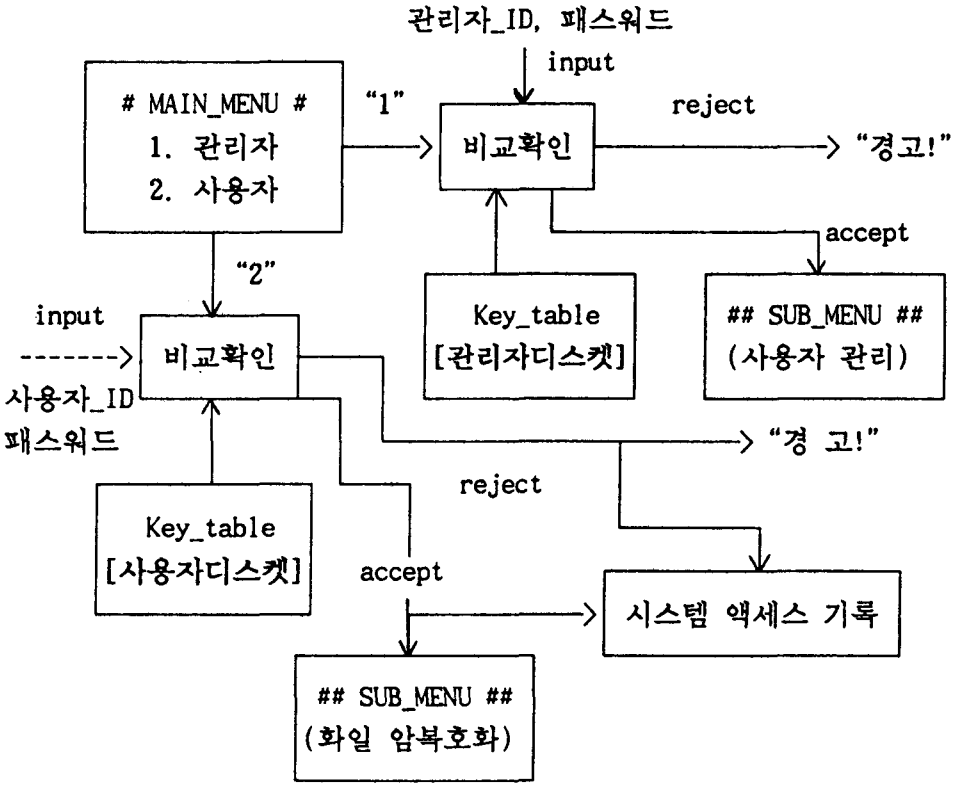
3. 설계 및 구현방향

상용 PC보안시스템은 보통 소프트웨어나 하드웨어를 병행하여 구성되어 있다. 전자는 PC내부에 친숙하거나 전문적인 지식을 가지고 있는 해커(Hacker)의 위협대상이 될 수 있으며, 후자의 경우는 하드웨어적인 장비가 뒤따르게 되므로 비용면에서 부담이 된다. 따라서 본 논문에서는 응용 소프트웨어로 구성된 시스템에서 노출되기 쉬운 사용자_ID 및 화일 패스워드를 관리하기 위하여 IC카드대신 우리주변에서 손쉽게 구할 수 있는 플로피 디스켓트에 키를 암호화하여 저장, 관리하는 방법을 사용하였다.

본 논문의 설계 및 구현방향은 패스워드 인증기법과 중요한 화일에는 삭제,변조등을 막기위해 화일속성 변경과 암호화 제어기법을 사용하였고 불법사용자를 추적하기 위해 시스템 사용자 액세스 기록기능을 구현하였다. 그리고 이 시스템은 MS-DOS환경하에서 한글코드 완성형으로 이루어진 IBM-PC호환 기종에서는 어디서나 사용할 수 있도록 Turbo-C언어로 구현하였다.

4. PC화일보호시스템 설계 및 구현

본 논문은 [그림 2]와 같이 여러가지 보안기법을 혼합하여 사용자_ID와 사용자 패스워드에 의해 시스템 액세스 인증을 받고 관리자와 사용자 업무를 분리시켜 관리자의 권한을 강화시켰으며 중요한 화일에 대해서는 화일속성 변경과 암호화 제어를 통하여 데이타 액세스를 제어하였다. 또 시스템 사용자의 액세스를 기록,유지하여 불의의 데이타 사고를 미연에 방지할 수 있도록 하였다.

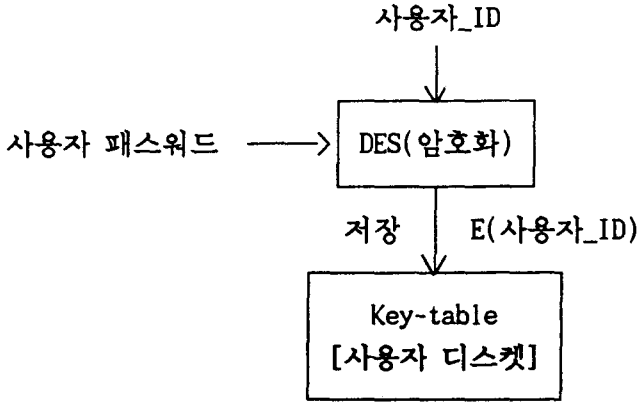


[그림 2] PC화일보호시스템 구성도

가. 시스템 액세스 인증(Authentication)

(1) 사용자 등록

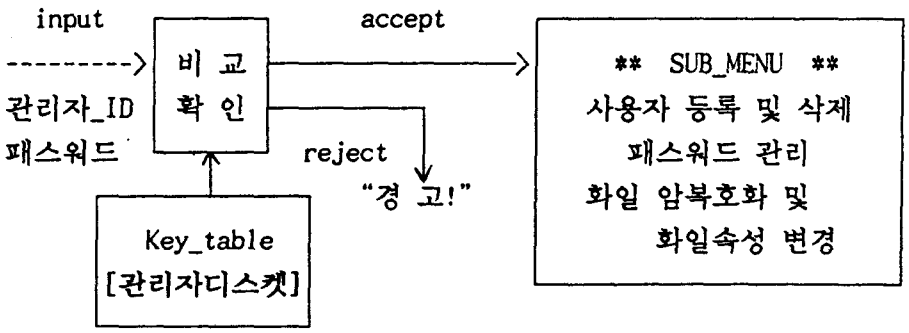
사용자 등록은 [그림 3]과 같이 관리자가 각 디스켓트에 개별적으로 입력한 사용자_ID를 사용자 패스워드에 의해 DES암호 알고리즘을 사용해서 암호화시켜 사용자 디스켓트 Key-table에 등록,저장시킴으로써 시스템 액세스시 인증이 가능하도록 하였다.



[그림 3] 사용자 등록

(2) 인증

이 시스템 인증은 MAIN-MENU에서 관리자와 일반사용자의 업무를 구분하여 번호를 선택함으로써 사용자는 관리자의 업무에 접근을 금지시키고 [그림 4]와 같이 처음 시스템 액세스시 사용자_ID와 패스워드를 입력함으로써 사용자 등록시 디스켓트 Key-table에 암호화되어 저장된 사용자_ID를 입력한 사용자 패스워드로 복호화하여 입력한 사용자_ID와 비교확인이 되면 다음 단계로 액세스를 허용한다.



[그림 4] 관리자(or 사용자) 인증

나. 화일 암호화제어

중요한 화일의 불법 액세스를 막기위하여 암호화시킴으로써 중요한 정보의 비밀성과 무결성을 보장한다. 그리고 본 논문은 암호화키의 생성,분배,관리에 중점을 두고 암호키 관리를 화일 패스워드와 사용자 패스워드에 의한 이중키 시스템을 사용하였다.

(1) 화일 암호키관리

PC에서 화일보호를 위한 암호화키 관리는 다음 3가지 사항에 중점을 둘 수 있다.

첫째, 하나의 키로 화일 전체를 암호화 시킨다.

이 방법은 키가 하나이므로 관리는 쉬우나 여러사람이 공유할 경우에는 노출이 되기 쉬우므로 전체 화일이 동시에 위협을 받을 수 있다.

둘째, 특정한 그룹단위로 키를 부여한다.

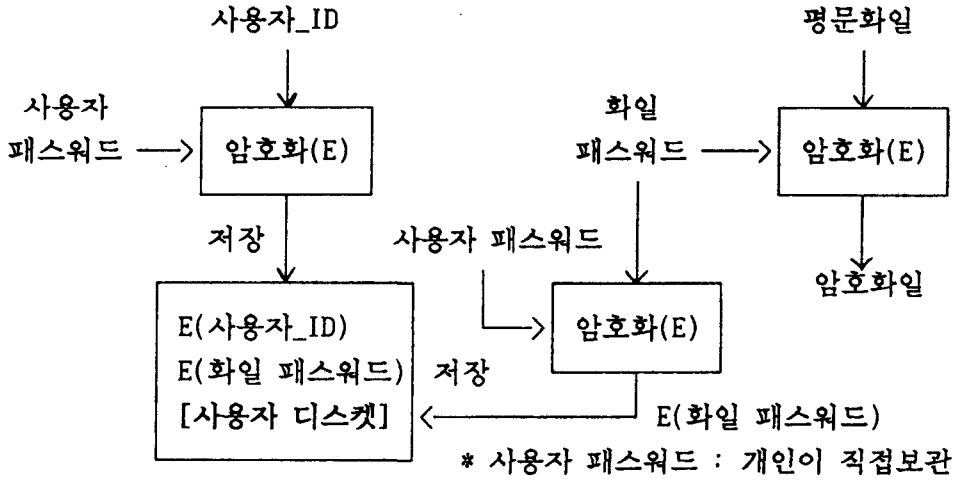
이 방법은 각 그룹에 대한 비밀성은 보장받을 수 있으나 첫번째 방법과 비슷한 위험

성에 노출되기 쉽고 여러그룹에 속한 사람은 여러개의 키를 보관해야 한다.

세째, 각각의 화일 단위로 키를 부여한다.

이 방법은 각 화일에 대한 비밀성을 최대한 보장받을 수 있고 다른 화일에 위험부담을 주지 않지만 한사람이 많은 키를 관리해야 하는 어려움이 뒤따른다.

이상과 같이 키관리는 시스템에 보관하거나, 개인이 직접 관리하거나, IC카드에 수록하여 사용하는 방법이 있는데, 시스템 관리는 해커의 우회적인 방법으로 노출이 가능하고, 개인이 직접 관리할 경우에는 보관하기 어렵고, 기록해놨을 경우에는 노출되기가 쉽다. 따라서 이러한 단점을 보완하기 위해서 비용이 많이 소요되지만 안전한 IC카드에 수록시켜 사용하는 방법이 등장하게 이르렀다. 그러나 본 논문에서는 [그림 5]처럼 경제적인 측면을 고려하여 IC카드 대신에 주변에서 흔히 구할 수 있는 플로피 디스켓트(floppy diskette)에 화일 패스워드를 암호화시켜 보관하고 이 화일 패스워드의 재암호화키인 사용자 패스워드는 개인이 직접 보관함으로써 안전한 키관리에 중점을 두는 혼용방법을 사용하였다. 그러나 디스켓트는 보관상 파손, 분실의 위험이 뒤따르지만 분실이 되었을 경우에는 개인이 직접 보관하는 사용자 패스워드를 알지 못하고는 사용이 어렵도록 하며 디스켓트 파손에 대해서도 하드커버의 디스켓(3.5인치) 등장으로 보관이 쉬워졌고 반드시 보관용 백업 디스켓트를 유지함으로써 파손이나 분실에 대비할 수 있다.

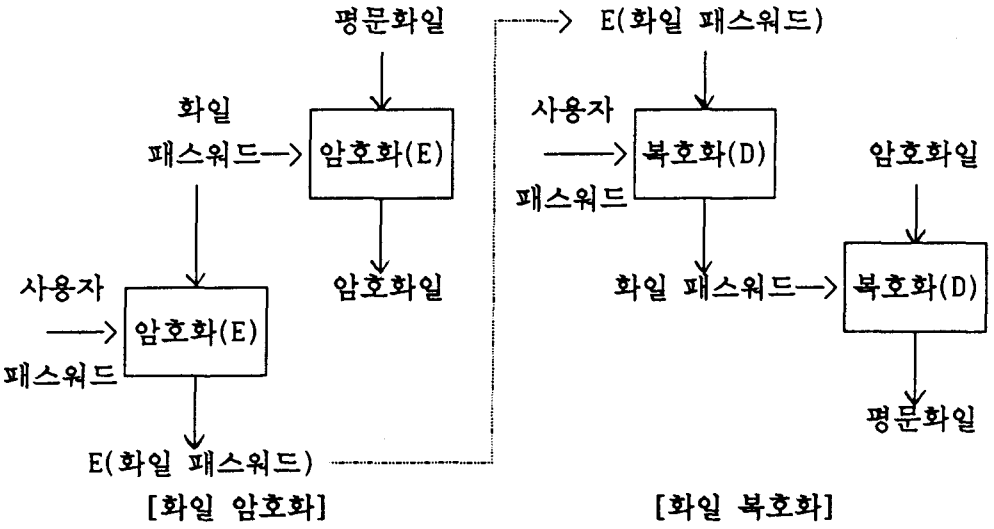


[그림 5] 화일 보호 암호화키 관리

(2) 화일 암복호화

화일암호화 루틴은 화일 패스워드를 8bit씩 integer값으로 받아들여 암호화키를 생성하고, 평문화일을 읽어들여 암호화 함수로 암호화시켜 8bit 크기의 integer값으로 암호화된 출력함수를 만들어내며, 복호화 루틴은 사용자 디스켓트 Key-table에 암호화되어 저장되어 있는 화일 패스워드를 사용자 패스워드로 복호화시켜 이 복호화된 화일 패스워드를 8bit씩 integer값으로 화일 복호화키를 생성하고, 암호화일을 8bit 크기의 integer값으로 읽어들여 복호화 함수로 복호화 시킨다.

이 암복호화 함수에 대한 키관리는 [그림 6]과 같이 각각의 중요한 화일을 암호화 시키고 자신의 보호를 위해서 사용자 패스워드로 재 암호화되어 사용자 디스켓트 Key-table에 보관시킴으로써 안전한 관리가 가능하였고 복호화 할때도 역으로 사용자 패스워드만 입력하면 각 화일에 대한 화일 패스워드가 자동으로 복호화되어 그 복호화된 화일 패스워드가 암호화된 데이타 화일을 복호화 시키게 된다.



[그림 6] 화일 암복호화키 관리

다. 화일속성 변경

각 화일에 은폐(Hidden), 읽기전용(Read_only) 기능을 부여시켜 사용자가 함부로 화일의 삭제 및 변조를 하지 못하도록 [그림 7]과 같이 f_attribute()로 구현하였다.

```
f_attribute(int argc, char *argv[])
{  union  REGS  inregs, outregs;
   int f_a;
   if (argc == 3)
     { switch(argv[2][0])
         case 'r' : f_a = 0x01;   break;  /* read_only */
         case 'h' : f_a = 0x02;   break;  /* hidden */
         case 'a' : f_a = 0x20;   break;} /* 정상환원 */
 }
```

[그림 7] f_attribute() 루틴

① 읽기전용(Read_only)

사용자는 화일에 대해 write기능은 없고 단지 화일을 읽을수만 있다.

② 은폐(Hidden)

중요한 화일을 삭제나 화일리스트상에 나타나지 않도록 화일의 이름

자체를 숨겨버리는 기능으로 사용상에 있어서는 삭제만 하지못할뿐
다른 기능은 은페이전의 경우와 똑같이 사용가능하다.

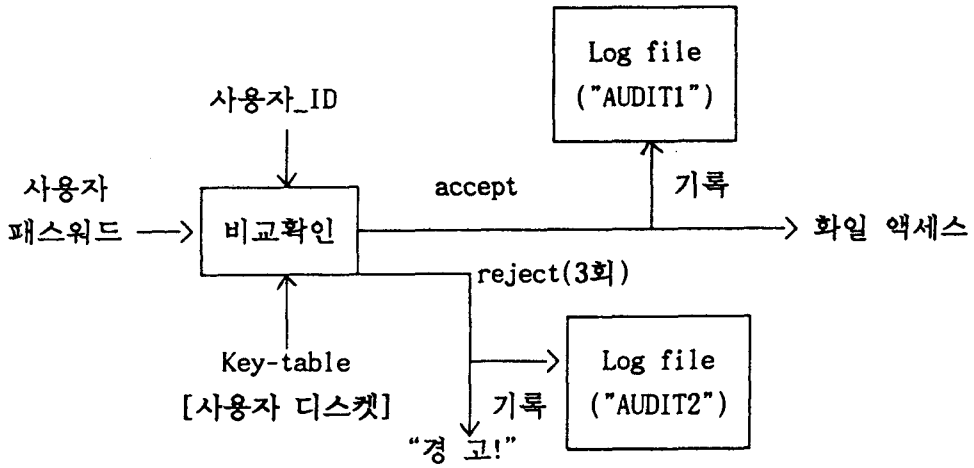
③ 원상태로 복귀(Archive free)
화일 속성의 변경내용을 다시 원상태로 액세스를 복귀시키는 기능

라. 시스템 사용자 액세스기록(Audit trail)

시스템을 안전하게 보호하고 불법사용자의 추적을 위해서는 사용자나 프로세스들의 액세스 기록, 각 객체들에 대한 액세스 형태를 점검할 수 있고 보호메카니즘의 우회적 불법침투를 발견할 수 있어야하며 사용자들의 불법우회 시도를 방지할 수 있어야 한다. 따라서 본 논문에서는 사용자 액세스기록 기능을 다음과 같이 구현하였다.

- 사용자 인증시에 사용자 기록
- 보안 위반에 대한 경고
- 불법 사용자의 액세스기록 및 시스템 사용금지

[그림 8]과 같이 사용자 인증시에 정상적인 사용자나 불법적인 사용자도 모두 각기 다른 log file에 사용자_ID와 액세스를 시도했던 시스템날짜와 시간을 기록하게 하였으며 또 사용자 인증시에 입력이 틀리면 "경고!" 메세지를 화면에 전개시키고 3회이상이면 시스템 액세스가 불가능 하도록 하였다.



[그림 8] 시스템 사용자 액세스기록 메카니즘

마. [ALT] 디렉토리 설정

지금까지 언급된 기능들은 데이타 보안에 있어서 가장 기본적이고 많이 사용되고 있는 보편적인 기법들이다. 그런데 CRYPTO-Chip이나 응용프로그램을 작성하지 않고 아스키문자 255번(CHR$(255))을 이용하여 서브디렉토리 또는 중요한 화일에 한 문자를 첨부시킴으로써 데이타 액세스를 제어하는 방법으로 실제로는 하나의 캐릭터를 차지하고 있지만 눈에 보이지 않으므로 불법 사용자에게는 화일 리스트상에 나타난 화일명이 다르므로 액세스가 불가능하게 할 수 있다.

Ⅴ. 결 론

PC의 증가로 발생되는 개인의 프라이버시 문제 및 자료의 변조에 따르는 부작용등으로 데이타 보안의 필요성이 강조되고 있어 본 논문에서는 이러한 문제점을 조금이나마 해소시켜 보고자 PC보안에 대한 개념을 정립해보고 상용 PC보안시스템 분석을 통하여 TURBO-C 언어를 사용, 사용자에게 메뉴방식을 제공함으로써 편리하고 안전한 PC화일보호시스템을 설계 및 구현하였다.

본 논문은 패스워드 인증기능, 화일 암호화 제어기능, 화일속성 변경기능, 사용자 액세스 기록기능등 기존의 PC보안 시스템과 유사한 방법으로 구현 하였지만 화일 암호화키 및 사용자 인증 패스워드를 관리하는데 있어서 CRYPTO-Chip이나 IC카드를 이용하고 있는 기존의 방법과는 달리 사용자_ID와 화일 암호화키(화일 패스워드)를 플로피 디스켓트라는 매체에 저장 보관시키고 사용자_ID와 화일 암호화키를 재 암호화시키는 사용자 패스워드는 사용자 자신이 직접 보관 함으로써 디스켓트를 분실했다 하더라도 데이타 노출이 쉽지 않도록 하는 혼용방법을 사용하였다.

이처럼 본 논문에서 제시한 시스템이 PC화일보호에 다소나마 도움이 되었으면 하는 바램이지만 디스켓트 부팅방지 및 화일 복사방지 기능을 연구 보완하여 더욱더 보안성 있는 PC화일보호시스템이 되도록 계속적으로 연구해야 할 것이다.

참 고 문 헌

1. D. E. Denning, "Cryptography and Data Security", Addison Wesley, 1982.
2. Charles P. Pfleeger, "Security in Computing", Prentice Hall, 1989.
3. Jennifer Sebery & Josef Pieprzyk, "CRYPTOGRAPHY : An Introduction to Computer Security", Prentice Hall, 1989.
4. NCSC(National Computer Security Center), "Personal Computer Security Consideration", NCSC Pub, WA-002-85, 1985.
5. Dennis D. Steinauer, "Security of Personal Computer Systems : A Management Guide", NBS Special Publication 500-120, 1985.
6. 남길현, "암호시스템의 특성과 활용", 정보과학회지, 1989, PP.55-64.
7. 남길현, 윤창섭, "국방 전산망 컴퓨터 보안에 관한 연구", 국방대학원, 1990.12.
8. 박용규, "퍼스널컴퓨터 보안시스템의 설계 및 구현에 관한 연구", 국방대학원 석사학위논문, 1991.
9. 신장균, 최은재, "화일보호와 안전한 운영체제", 정보과학회지, Vol.7, NO.5, 1989, PP.35-41.