시스템 종속적인 키(Key)를 이용한 PC 화일 보호 기법

박 영 선, 김 화 수
국방대학원 전자계산학과

PC File Protection Scheme using System-Dependent key

Young-Sun Park, Hwa-Soo Kim
Dept. of Computer Science, National Defense College

요 약

PC 사용의 확산에 따라 PC 화일 보호의 요구가 대두되고 있으나, 기존의 사용자 단일 키에 의한 암호화 제어 기법은 키의 노출이 용이하고, 인가된 사용자에 의한 비밀화일의 불법 도용을 방지하기 어려운 취약점이 있다.

이러한 문제점을 개선하기 위하여 제안하고자 하는 이중키(시스템 종속적인 키와 사용자 키)에 의한 암호화 제어는 사용자 키를 이용하여 입력된 데이타를 암호화하고, 암호화된 데이타를 시스템에 종속적인 키를 이용하여 다시 암호화해서 화일에 저장한다. 제안된 기법의 특징은 이중키를 사용함으로서 (i)키 공격에 대한 저항성 증가, (ii)키 노출의 위험성 감소, (iii)인가된 사용자의 불법적인 화일 도용을 방지하는 것이다.

이중키에 의한 암호화 제어 기법은 정보의 비밀성 보호가 크게 요구되는 조직이나 기관에 적용하는 것이 효과적이며, 이중키의 생성 및 관리, 인증 및 접근 제어를 포함한 계층적인 제어를 위한 추가적인 연구가 요구된다.

I. 서 론

컴퓨터의 이용이 대중화되면서 PC를 사용한 대량의 자료가 생산, 처리, 관리되고 있다. 종전에는 개인 업무 처리에 주로 사용되던 PC가 이제는 자료의 분산처리 추세에 편승하여 사무처리 및 컴

퓨터 통신망의 최종시스템(End System)으로 그 사용이 날로 확산되고 있다. 이러한 PC의 확산은 컴퓨터 대중화를 촉진한 반면 개인의 프라이버시 침해나 정보의 변조, 훼손, 절취, 부정 작취 등의 정보 범죄 유발를 용이하게 하고, 피해의 규모를 크게하거나 범위의 광역화를 초래할 우려가 있다. 이에 따른 대비책으로 PC의 화일 보호 시스템이 큰 관심거리로 대두되고 있으나 그 중요성에 비추어 연구사례는 비교적 적은 편이다.

PC의 화일 보호 시스템에서 패스워드나 엑세스 제어에 의존하는 소극적 보호 대책으로는 여러 형태의 공격으로부터 취약하므로 주로 암호화 제어(Cryptographic Control) 등의 적극적인 매카니즘을 사용하고 있다[1]. 암호화 제어는 키(Key)를 사용해서 평문자료를 암호문으로 바꾸어 화일에 저장하므로서 불법 사용자로부터 화일을 안전하게 보호하는 것이다. 암호화 제어는 키에 의해서 보안성을 보장받으므로 이 키의 관리와 분배가 중요한 문제가 된다. 기존의 암호화 제어는 사용자 키(단일 키)만을 암호화에 사용함으로서 키가 노출되기 쉽고, 인가된 사용자에 의한 화일의 불법 도용(절취, 유출 등)에 취약하기 때문에 화일 보호 기법으로는 미흡하다. 이에 비해 보안 담당자가 관리하는 시스템에 종속적인 키(시스템키)와 사용자가 동적으로 관리하는 키(사용자키)의 이중키에 의한 암호화(하나의 키로 암호화된 자료를 다른 키로 다시 암호화하는 방법)를 사용하면 키 관리가 복잡해지기는 하지만 이러한 문제점을 개선할 수 있다.

PC에서 사용되는 운영체제는 비교적 단순하고 공개되어 보안성이 낮으므로 운영체제가 지원하는 화일 보호 기능은 취약점이 많으며, PC 가격은 저렴하여 고가의 보안 시스템 도입에 장애가 되고 있고, 또한, 다수의 동일 특성을 갖는 시스템이 존재하므로 물리적인 보안이 어렵다. 본 논문에서는 PC의 이러한 특성에 부합되는 소프트웨어적인 구현이 가능하고 물리적인 보안이 곤란한 환경에서도 안전한 화일 보호가 가능한 이중키에 의한 화일 보호 매카니즘을 제안하고자 한다.

컴퓨터의 화일 보호 시스템은 정보의 비밀성(security), 무결성(integrity), 이용성(availability)의 3가지 중요한 요소가 있는데[2] 본 논문에서는 무결성과 이용성의 보장은 비밀성 보장과는 독립적으로 운영체제의 기능을 통해 달성 가능한 것으로 가정하고 확고한 비밀성의 달성에 중점을 두었으며, PC 화일 보호 시스템 설계시 암호화 알고리즘은 DES를 사용하였다.

II. PC 화일 보호 기법

PC의 화일 보호 기법은 분류 방법에 따라 물리적인 보호 기법으로부터 하드웨어 또는 소프트웨어적인 보호 기법까지 여러가지를 고려할 수 있지만, 대부분 인증을 위한 패스워드 제어 기법, 해당 화일의 사용 범위에 대한 권한을 제어하는 엑세스 제어 기법, 화일을 암호화하여 저장하는 암호화 제어 기법의 범주에서 설명될 수 있다.

2.1 패스워드 제어 기법

불법 사용자를 식별하기 위한 인증 방법으로 주로 단방향 함수를 이용해서 평문의 패스워드를 암호화하여 시스템에 저장해 놓고, 사용자로부터 입력 받은 패스워드를 암호화한 상태에서 저장된 암호문과 동일한지 비교함으로서 사용자를 인증할 수 있다[3].

이 기법은 보호 화일에 대한 불법 사용자의 접근을 포괄적으로 통제하는 수준의 제어로서 구조가 간단하고 구현이 용이한 반면, 시스템 고장으로 불법 사용자의 접근이 가능해지거나 보안 관리자가 불순한 마음을 품었을 때는 안전하지 못하며[4], 운영체제의 보안성이 낮을 경우 시스템 화일의 변조나 인증 절차의 우회 등을 통한 불법 접근 위협에 취약하다.

2.2 엑세스 제어 기법

화일은 데이타의 저장 매체로서 해당 화일에 대한 적법한 사용자임이 인증되었다 할지라도 권한 없는 삭제, 수정, 그리고 첨가로부터 보호되어야 한다. 이 목적을 위해 엑세스 제어 기법이 필요하다[3].

엑세스 제어를 위해 화일에 대한 사용자들의 엑세스 권한 테이블을 시스템에 저장해 놓고, 사용자 식별자(ID)를 가지고 그 테이블을 검색해서 해당되는 엑세스 권한 범위를 부여함으로서 계층적인 제어를 달성한다.

엑세스 제어 기법은 다양한 사용자의 자격에 따른 여러가지 제어범위를 설정할 수 있는 장점이 있는 반면, 엑세스 권한을 명세화해 놓은 정보는 절대적으로 안전해야 한다. 이를 위해 권한 테이블을 암호화해서 저장하는 방법 등을 사용하고 있으나, 운영체제의 보안성이 낮을 경우 패스워드 제어 기법과 같은 취약성이 있으며 근본적으로 화일이 투명한 상태로 존재하므로 안전한 화일 보호에는 미흡하다.

2.3 암호화 제어 기법

화일에 데이타가 저장되기 전에 평문 데이타가 암호화 키에 의해 암호문으로 변환되어 저장되므로서 복호화 키를 모르는 불법 사용자가 화일에 접근했다 하더라도 해당 화일의 내용을 알지 못하도록 해서 데이타의 비밀성을 보장하는 기법이다. 따라서 암호화 제어 기법은 다른 어느 기법보다 화일 보호의 목적에 부합되는 기법으로 볼 수 있다.

암호화 시스템은 키에 의존해서 보안성을 보장 받기 때문에 키의 생성, 분배 그리고 관리하는 것이 중요한 문제이다. 암호화 키를 관리하는 것은 사용자에 의한 관리와 시스템에 의한 관리를 생각할 수 있는데, 전자의 경우에는 되도록 짧은 길이의 키를 선호하므로서 비도를 낮게할 우려가 있고, 키를 분실시에는 화일의 복원이 곤란한 단점이 있는 반면 키의 공격으로부터의 보안성은 높다.

후자의 경우에는 비밀키를 시스템 내에 저장하기가 곤란하고, 키에 대한 공격에 취약한 반면 비도가 높은 긴 길이의 키에 대한 관리가 용이하고 분실의 우려가 없다. 이 두가지 방법의 장단점을 보완해서 하드웨어적인 방법(마그네틱 카드)으로 키를 생성, 관리하면 상기의 단점을 제거하고 효과적인 키 관리가 가능한 반면 추가적인 장치와 비용이 소요된다[3].

상기 기술한 것을 요약하면 화일 보호 기법들은 불법 사용자의 집중적인 공격에 취약점을 갖는 단일 기법에 의한 운용을 지양하고 복합적인 계층적 제어 구조로 통합하여 보다 효과적인 보호를 달성할 수 있으며, 어느 한 기법의 취약점을 다른 기법의 강화로 보완할 수 있다. 패스워드 기법이나 엑세스 제어 기법은 제어에 요구되는 데이타가 비록 암호화되어 있기는 하지만 시스템 화일 내에 존재하므로 암호화 기법 보다는 불법 사용자의 공격에 취약하다. 특히 PC의 운영체제는 시스템 특성상 구조가 간단하고 비교적 널리 공개되어 있어 비밀성이 낮으므로 시스템 화일 내용의 변조나 절취를 통해서, 또는 운영체제 일부를 변조해서 제어 구조를 우회하므로서 화일에 접근할 가능성이 크다. 따라서 PC 화일 보호 시스템에서는 패스워드나 엑세스 제어 기법은 인증을 위한 보조적인 화일 보호에 사용하고, 화일의 비밀성 보장을 위해서 암호화 제어 기법을 더욱 강화해야 함을 알 수 있다.

III. 시스템 종속적인 키를 이용한 PC 화일 보호 기법

기존의 암호화 화일 보호는 사용자가 입력하는 키를 가지고 평문 자료를 암호화하여 화일로 저장한다. 부가적으로 시스템내 존재하는 사용자 키가 투명한 형태로 시스템내에 존재하는 것을 방지하기 위해 사용자 키를 암호화해서 저장하는데 사용하는 마스타 키가 있으나 이는 데이타 암호화에는 관여하지 않는다[5]. 결국 사용자 단일 키에 의해 암호화된 화일이 생성되는 것이며, 사용자 키가 노출시 해당 화일의 보호는 파괴된다.

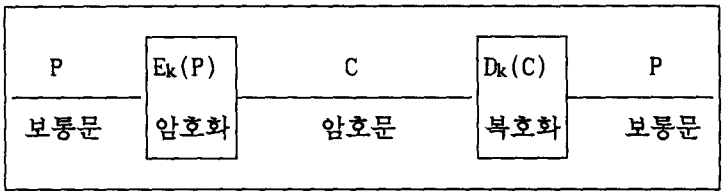
PC는 개인 업무 처리, 사무처리, 컴퓨터 통신망의 최종 시스템 등의 다양한 요구를 수용해야 하기 때문에 항상 통제된 비밀작업만을 전담 수행하기가 곤란하다. 따라서 평상시는 평문으로 입.출력되는 정상적인 화일 시스템을 유지하고 있다가 비밀작업이 요구될시 암호화 환경을 설정해서 암호화 화일에 의한 입.출력을 수행하고, 비밀작업이 종료되면 다시 평상시 상태로 회복돼야 한다. 이러한 요구를 수용할 때 단일 키에 의한 암호화 시스템은 빈번한 업무 전환에 따른 사용자 키의 노출 가능성이 높고, 비밀 화일의 인가된 사용자가 불법적으로 이 화일을 도용하고자 할 때 그 대비책이 없다. 이런 문제에 대한 해결책으로 이중키(시스템 종속적인 키와 사용자 키)에 의한 화일 암호화 시스템을 생각할 수 있다.

3.1 이중키 구조 및 특징

암호화 키를 이용 평문을 암호문으로 변환하고, 복호화 키를 사용 암호문을 평문으로 재생하는

암호 시스템을 구성하는 요소는 <그림 3-1>과 같다[3].

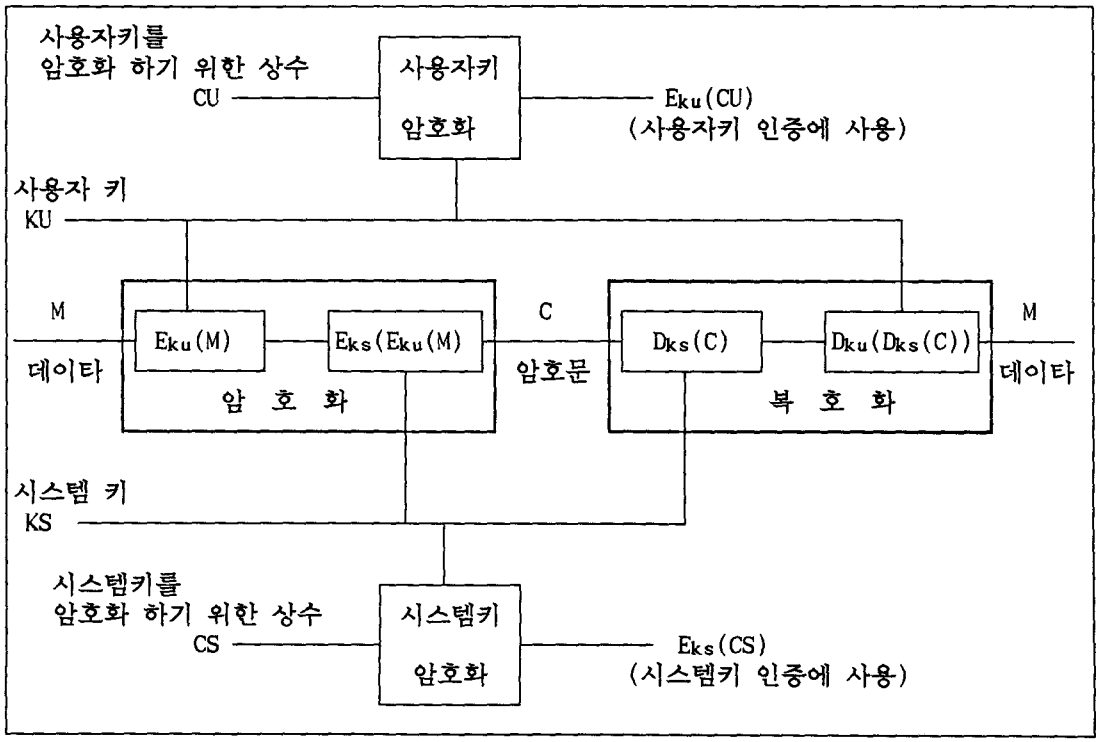
- ◆ 보통문 (Plaintext : P)
- ◆ 암호문 (Ciphertext : C)
- ◆ 키 (Key : K)
- ◆ 암호알고리즘 (Encryption Algorithm : E_k), $E_k(P) = C$
- ◆ 복호알고리즘 (Decryption Algorithm : D_k), $D_k(C) = P$



<그림 3-1> 암호 시스템

암호 알고리즘으로 사용하는 DES는 미국 상무성 표준국에서 정부표준 암호시스템으로 1977년 채택했으며, IBM의 Tuchman 등이 만든 Lucifer cipher를 기초로 한 block product cipher로서, 64bits의 평문 데이타가 56bits의 입력 키에서 생성된 16가지의 키에 의하여 16회의 암호계산 단계를 거쳐 64bits의 암호문을 작성한다[6]. DES는 대칭형 암호알고리즘으로서 암호화 및 복호화에 동일 키를 사용하며, 수행 속도가 빠르고 크기가 작기 때문에 PC 화일 암호화 알고리즘으로 적합한 것으로 판단된다.

제안된 이중키에 의한 암호 시스템을 DES를 이용해서 구현하면 <그림 3-3>과 같다.



<그림 3-3> 이중키 암호화 시스템

암호화 과정은 다음과 같다.

1. 평문 데이타(M)가 사용자키(KU)에 의해 암호화 : $E_{ku}(M)$
2. 사용자키에 의한 암호문($E_{ku}(M)$)이 시스템키(KS)에 의해 암호화 : $C = E_{ks}(E_{ku}(M))$
3. 암호문(C)을 화일에 저장

복호화 과정은 다음과 같다.

1. 암호문(C)이 시스템키(KS)에 의해 복호화 : $D_{ks}(C)$
2. 시스템키에 의한 복호문($D_{ks}(C)$)이 사용자키에 의해 복호화 : $M = D_{ku}(D_{ks}(C))$
3. 복호화된 평문이 사용자에 의해 사용됨

시스템 내에 상주하면서 사용자가 인지하지 못한 가운데 화일의 암호화 및 복호화에 관여하는 시스템키는 보안 담당자가 관리하는 시스템 종속적인 키이다. 시스템키의 생성은 보안 담당자가 조직 내에 있는 다수의 PC를 대상으로 서로 다른 키를 갖도록 랜덤하게 생성한다. 시스템 키의 분배는 시스템이 부팅될 때 보안 담당자에 의해 수동적으로 이루어지고, 시스템이 꺼지는 것과 동시에 사라진다. 생성된 키는 문서화된 다음 비밀 문서 관리 규정에 의해 조직의 책임자가 관리하게 된다.

사용자키는 화일의 성격에 따라 사용자가 동적으로 생성하고 분배 및 관리한다. 이때 보안 담당자와는 독립적으로 생성되도록 유의해야 하며, 그룹이 하나의 키를 생성해서 그룹 단위의 화일 보호 및 공유도 가능하다.

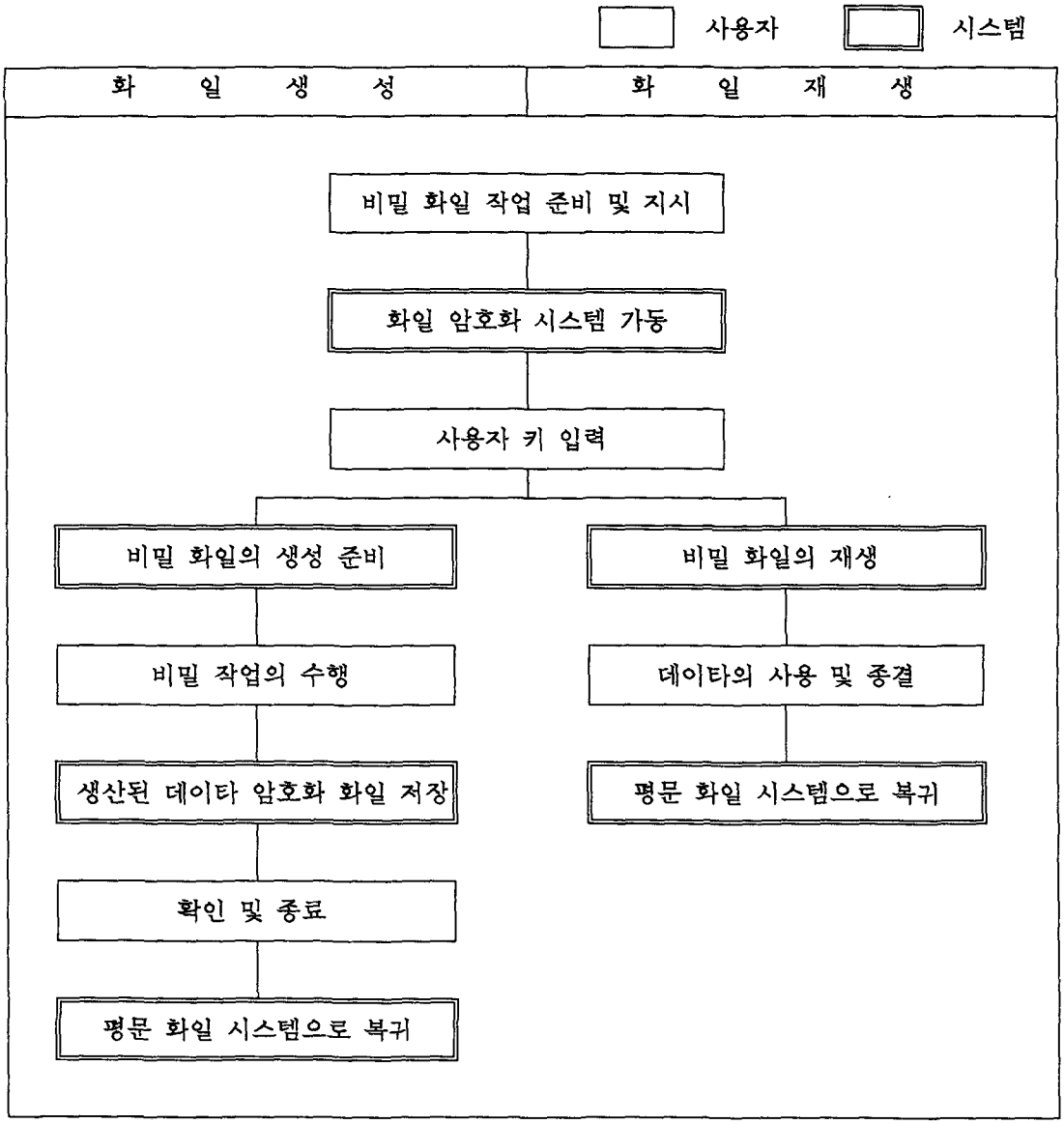
화일의 암호화는 키에 의존하므로 착오로 잘못된 키 값을 입력시는 해당 화일의 복호가 불가능함으로 키의 인증은 중요한 역할은 한다. 키의 인증은 일방향 함수에 의한 방법을 사용한다. 사용자키(KU)는 암호화를 위해 키 입력시 지정된 상수(CU)를 DES의 입력 데이타 값으로 하여 사용자 키를 사용해서 암호화된다. 암호화된 키 값($E_{ku}(CU)$)은 해당 화일에 저장되어 있다가 복호시 다시 입력되는 키를 동일한 방법으로 암호화한 상태에서 비교함으로서 인증된다. 시스템 키도 동일한 방법으로 인증되는데 다만 암호화된 키 값이 주기억장치 내에 있는 임시 저장 장소에 존재하게 된다.

이와 같은 이중키의 특징은 첫째, 하나의 데이타에 암호 알고리즘을 이중으로 적용해서 키의 길이를 2배로 확장한 것과 같은 효과를 갖기 때문에 비도를 증가시키게 된다. 둘째, 두개의 독립적인 키가 운용되므로 키의 노출에 따른 암호 시스템 파괴의 위험성을 최소한으로 감소시킨다. 세째, 시스템 종속적인 키가 존재하므로서 인가된 사용자라 하더라도 해당 시스템을 벗어나서는 암호화된 화일을 복원할 수 없어 인가된 사용자에 의한 불법 도용을 방지할 수 있다.

3.2 암호화 화일 보호 매카니즘

암호화 화일 보호는 비밀 데이타가 화일에 기록되고 판독될 때 특정한 키와 암호화 알고리즘에 의해 블럭 단위로 암호화 및 복호화되도록 하여 비인가자가 비밀 내용를 알 수 없도록 함으로서 달성된다. 이상과 같은 매카니즘은 화일 보호를 위한 화일 시스템과 정상적인 화일 시스템이 병존하면서 사용자 요구에 따라 반응하는데, 이를 화일 생성 과정과 화일 재생 과정으로 구분하여 표시하면

<그림 3-4>와 같다.



<그림 3-4> 화일 보호 매카니즘

3.2.1 화일 생성 과정

1. 사용자가 비밀작업을 할 것을 결정하면 보안에 필요한 외부 환경을 정돈하고 필요한 참고자료 등 작업준비를 한 다음 PC에 비밀 화일 보호 시스템을 가동시킨다. 비밀 화일 보호 시스템은 화일에 입력되는 모든 데이타는 암호화 과정을, 화일에서 출력되는 모든 데이타는 복호화 과정을 거치도록 기존의 화일 시스템을 수정한다.

2. 사용자 키를 생성하여 화일 보호 시스템의 요구에 의해 입력한다. 입력된 키는 임시 변수에

저장된 후 인증을 위해 암호화되어 해당 화일에 저장되며, 데이타 암호화에 사용된다. 사용자키에 의해 암호화된 데이타는 임시 메모리에 저장된 시스템 키에 의해 다시 암호화된다.

3. 응용 프로그램을 이용해서 데이타를 평상시 작업 처럼 처리하면 사용자가 인지하지 못한 가운데 화일로 출력되는 모든 데이타는 암호화되어 저장된다.

4. 작업을 완료하고 화일의 생성을 확인한 후 화일 보호 시스템을 종료하면 기존의 정상적인 화일 시스템으로 복귀된다.

3.2.2 화일 재생 과정

1. 첫째 과정은 화일 생성의 경우와 동일하다.

2. 사용자 키가 입력되면 암호화한 다음 화일에 저장된 암호화된 키 값과 비교하여 틀리면 화일 재생을 거부하며, 일치하여 인증이 되면 키를 임시 변수에 저장하고 시스템 키에 의해 복호화된 데이타를 다시 복호화하여 평문으로 전환한다.

3. 평문으로 전환된 화일의 데이타는 응용 프로그램에 의해 처리된다. 수정, 첨가된 데이타가 화일로 재출력 될 때에는 생성 과정과 같은 절차를 따라 암호화되어 저장된다.

4. 작업이 완료되면 기존의 정상적인 화일 시스템으로 복귀한다.

3.2.3 응용 분야

이중키에 의한 암호화 제어는 강력한 암호 매카니즘을 제공한 반면 키의 관리가 어렵고, 시스템에 종속적인 키를 두므로서 정보의 공유화를 곤란하게 할 우려가 있다. 따라서 정보가 노출 되었을 경우 그 피해의 규모가 크고 광범위하게 발생하는 조직이나 기관에서 사용할 때 효과적이다. 또한 주로 일반 업무를 수행하면서 필요시 비밀 업무를 수행해야 하는 시스템은 외부환경을 통제해야 하는 물리적 보안이 어렵고, 키 노출의 가능성 높기 때문에 이중키를 사용하면 효과적인 정보 보호를 달성하면서 일반 업무의 수행을 보장할 수 있다.

이중키를 마그네틱 카드 등의 하드웨어적인 방법으로 관리할 수 있다면, 다양한 키를 안전하게 생성할 수 있으므로 정보의 공유 문제나 키 관리의 문제를 해결할 수 있어 응용 범위를 확대할 수 있다.

IV. 결론 및 추가 연구 사항

본 연구에서는 PC의 화일 보호와 관련하여 기존의 단일키에 의한 암호화 제어의 취약성을 개선하고 비밀성 보장이 강화된 이중키에 의한 시스템 종속적인 암호화 제어 기법을 제안하였다.

제안한 이중키에 의한 화일 암호화 시스템은 사용자 키를 사용하여 입력된 데이타를 암호화하고, 암호화된 데이타를 다시 시스템에 종속적인 시스템 키를 사용하여 다시 암호화해서 화일에 저장한다. 시스템키는 해당 조직의 보안 담당자가 각 PC별로 랜덤하게 생성해서 사용자와 독립적으로 PC 가동 초기에 입력하므로서 각 PC가 서로 다른 키를 갖게되어 사용자가 인지하지 못하는 시스템 종속적인 키가 된다. 따라서 사용자가 화일을 불법적으로 복사해서 소지한다 하더라도 최초 비밀화일를 생성한 PC와 보안 담당자의 키가 없이는 복호가 불가능하게 된다. 즉 키를 이중화함으로서 키 공격에 대한 저항성 증가, 키 노출의 위험성 감소, 인가된 사용자의 불법적인 화일 도용을 방지할 수 있게 되었다. 이것은 평문화일과 비밀화일이 동일한 환경하에서 사용가능하고, PC의 다양한 업무를 수용하면서 비밀화일에 대한 보호가 달성될 수 있음을 의미한다.

향후 PC의 화일 보호 기법을 더욱 발전시키기 위해서는 이중키의 생성 및 관리 전략, 사용자 인증과 엑세스 제어 기법이 복합된 계층적 화일 암호화 연구, PC 특성에 부합되는 보안 요구 조건의 연구 등에 관심을 갖고 연구되어야 할 것이다.

V. 참 고 문 헌

1. 차승렬, "PC-Xinu 운영체제에서의 안전한 화일시스템 설계 및 구현", 국방대학원 석사학위논문, pp.1, 1990.

2. John McLean, "The Specification and Modeling of Computer Security", IEEE Computer, January 1990, pp.9-16.

3. 남길현, 윤창섭, "국방전산망 컴퓨터보안에 관한 연구", 국방대학원, pp.29-33, 1990.

4. 이필중, 문희철, "패스워드 시스템의 보안에 관한 고찰", 통신정보호호학회지, 제1권, 제1호, pp.111, 1991.

5. 염흥렬, "컴퓨터 통신망에서의 암호키 생성, 분배, 그리고 관리방식", 통신정보보호학회지, 제1권, 제1호, 1991

6. 이경석, "Cryptosystem의 기법과 동향분석", 통신정보보호학회지, 제1권, 제1호, pp.134, 1991