韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

패스워드 시스템의 보안에 관한 고찰

이 필 중*·문 희 철*

시 분할 원격 접근 컴퓨터 시스템이나 컴퓨터 네트워크에서 사용자의 인증(authentication)을 위해 패스워드가 가장 널리 이용되고 있다. 일반적으로 패스워드는 시스템에 들어가고자 하는 사용자를 인증하거나 시스템을 이용중인 사용자에 대해 자료(file)의 접근을 제한하는 용도로 이용된다. 따라서 패스워드 시스템이 불안전하다면 시스템이 위험에 빠지고 귀중한 정보가 노출 또는 변경될 수도 있으므로 패스워드의 보안은 아주 중요한 문제이다.

이 글에서는 현재 사용되는 시스템들의 패스워드 보안현실을 알아보고 그에 대한 문제점을 지적하며 보다 안전한 패스워드 시스템의 보안에 대한 방안을 고찰한다.

1. 서 론

컴퓨터 보안분야에서 사용자의 인증을 위해 가장 널리 사용되는 방법으로 패스워드의 사용을 들 수 있다. 사용자의 인증에는 그 사람 만의 특징(목소리, 지문 등)이나 그 사람만의 소유물(카드 등) 또는 그 사람만이 아는것(패스워드 등)으로 그 사람을 인증하는 세가지 방법이 있다[1]. 이중 하나인 패스워드란 그 사용자만 알고 있는 문자들의 집합이며, 이를 인증에 이용하는 시스템을 패스워드 시스템이라 한다. 현재 대부분의 개인용 컴퓨터, 시 분할 원격 접근 컴퓨터 시스템(time sharing remote access computer system)이나 컴퓨터 네트워크에서는 사용자가 시스템에 자신의 ID와 패스워드를 입력함으로써 자신을 인증한다.

* 정회원, 포항공과대학 전자전기공학과

일반적으로 패스워드는 두가지의 다른 용도를 가지고 있다. 첫째는 시스템에 들어 가고자 하는 사용자를 인증하는 것이고 둘째는 시스템을 이용중인 사용자에 대해 자료(file)의 접근을 제한하는 용도이다. 따라서 시스템에 불법으로 침입하거나 허가되지 않은 데이타를 읽거나 수정하고자 하는 자는 반드시 시스템이 인증할 수 있는 패스워드를 알아 내야 한다. 만약 패스워드 시스템에 헛점이 있다면 시스템이 위험에 빠지고 귀중한 정보가 노출되거나 변경될 수도 있으므로 패스워드의 보안은 아주 중요한 문제이다. 그러므로 시스템의 관리자나 사용자는 패스워드가 노출되지 않도록 안전한 방법을 강구해야 한다.

본고에서는 현재 사용되는 시스템의 패스워드 보안의 현실을 알아 보고 그에 대한 문제점을 지적하며, 보다 안전한 패스워드 사용 및 관리상의 방안을 제시하고자 한다.

2. 본 론

가. 패스워드 시스템의 개요

패스워드 시스템에서는 사용자가 자신의 식별자(identifier, ID)와 패스워드를 입력하여 자신을 인증한다. 모든 사용자들의 식별자와 패스워드는 시스템내에 저장되어 있고 시스템은 입력된 식별자와 패스워드를 저장되어 있는 것과 비교한다. 비교결과 올바른 식별자와 패스워드가 입력되었을 경우에만 사용자에게 시스템이나 화일에 접근할 수 있는 권한을 준다.

컴퓨터 보안 문제를 해결하기 위해 패스워드를 사용하려 했을 때 처음에는 다음과 같은 방법이 이용되었다. 즉 식별자와 패스워드를 패스워드 화일에 저장하고 시스템 관리자를 제외한 모든 이에게 그 화일에 대한 접근을 제한하는 것이다.

그러나 이 방법은 시스템의 고장이나 시스템 관리자의 패스워드가 노출되는 등의 경우에 패스워드 화일이 노출될 수 있고 그때마다 모든 사용자들이 패스워드들 바꿔야 하는 문제가 있었다. 더욱 큰 문제는 시스템 관리자 자신에 대해서는 아무런 제한 조치를 할 수 없고 그가 그만둘 때 패스워드 화일을 복사해 가지고 나갈 수도 있다는 점이다.

그래서 이 문제를 해결하기 위해 일방함수(one-way function)를 이용한 새 방법이 고안 되었다[2]. 이 방법은 그림 1에서와 같이 패스워드를 입력으로 하여 일방함수를 계산한 결과를 식별자와 함께 패스워드 화일에 저장하는 것이다. 일방함수란 한 방향으로의 계산은 쉬운 반면 반대방향의 계산은 불가능한 함수를 말한다. 따라서 P_i를 이용하여 $F(P_i)$를 계산하기는 쉬워도 $F(P_i)$로부터 P_i를 계산해내기는 거의 불가능하다.

사용자가 식별자와 패스워드를 입력하면 시스템은 그 패스워드를 일방함수를 거쳐 저장되어 있는 것과 비교하여 사용자를 인증한다. 그림 2.는 이러한 인증방법을 설명한다. 전의 방법과 달라진 점은 역함수의 계산이 불가능하므로 패스워드 화일 자체에 대한 보안이 불필요하게 된 것이다. 왜냐하면 패스워드 화일을 공개해도 그 화일로부터 다른 사람의 패스워드를 알아낼 수 없기 때문이다.

일방함수로는 보통 DES(Data Encryption Standard) 알고리즘을 이용한다[3, 4]. DES는 8바이트의 데이타와 8바이트의 키이(key)를 입력하면 8바이트의 암호문을 출력하는 함수로 생각할 수 있다. 일반적으로 암호 알고리즘은 일방함수로도 사용이 가능하며 DES를 일방함수로 사용할 때에는 패스워드를 키이로 사용하여 어떤 정해진 상수를 암호화하여 그 결과를 패스워드 화일에 저장한다. 예를

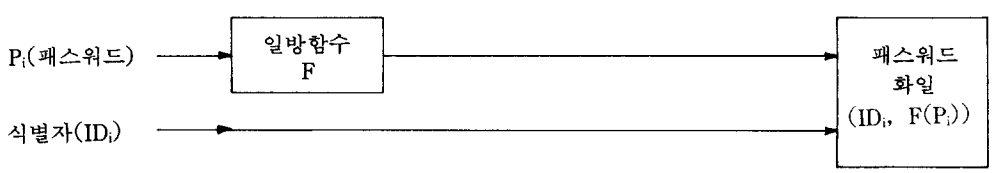

그림 1. 패스워드의 저장

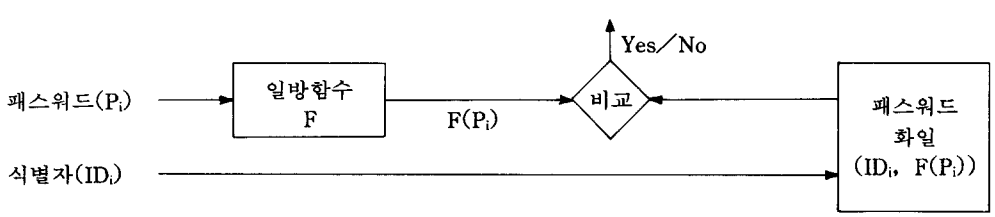

그림 2. 패스워드의 인증

들면 UNIX 시스템에는 패스워드를 비롯하여 시스템이 각 사용자에 대하여 필요한 모든 정보를 포함하고 있는 /etc/passwd라는 화일이 있다. 화일 내용중 패스워드에 해당하는 부분은 일방함수인 crypt로 처리되어 있어 읽어도 해독하기가 거의 불가능하다[5]. 그러므로 누구나 /etc/passwd 화일을 읽고 프린트하는 것이 허용된다. 사용자가 로그인할 때 마다 단말기에서 입력한 패스워드는 암호화되고 이미 /etc/passwd 안에 만들어져 있는 패스워드와 비교된다.

나. 일반적인 패스워드 시스템 보안의 위협

패스워드 시스템 보안의 위협이란 사용자의 패스워드가 불법적으로 노출되는 것을 말한다. 시스템에 불법침입하려는 자는 아래의 세가지 방법으로 사용자의 패스워드를 알아낼 수 있다.

첫째, 시스템의 패스워드 화일을 읽어내는 방법이 있다. 패스워드 화일은 사용자들의 패스워드와 식별자를 저장한 화일로서 만약 노출되면 시스템과 모든 사용자들의 자료는 위험에 빠지게 된다. 따라서 패스워드 화일은 일반 사용자에게 접근을 제한하며 오직 보안 관리자만이 권리를 갖게 한다. 그러나 시스템의 고장이 생겨 일반 사용자들도 패스워드 화일에 접근 가능하다거나 보안관리자가 불순한 마음을 품었을 때에는 이와같은 패스워드 시스템은 전혀 안전하지 못하다[6]. 보다 확실한 방법은 패스워드를 일방함수를 사용하여 그 결과를 식별자와 함께 화일에 저장하여 패스워드 화일이 노출되어도 안전을 유지하게 하는 것이다. 이 방법은 입력된 패스워드에 일방함수를 적용하여 그 결과를 저장된 것과 비교함으로써 사용자의 인증을 한다.

둘째, 사용자와 시스템간에 패스워드를 주고 받는 통신을 도청할 수 있다. 통신회선의 도청은 엿듣기만하는 수동적 라인 태핑(passive linetapping)과 적극적 라인 태핑(active linetapping)이 있다[7]. 만약 보안 관리자가 패스워드 시스템의 도청의 위험이 크다고 판정하면 통신되는 패스워드는 입력장소에서 암호화되어 비교 장소까지 전달되는 방법을 취해야 한다.

세째, 패스워드가 부주의하게 만들어져 쉽게 추측할 수 있는 경우이다. 실제로 사용자들은 자신들과 연관되거나 흔히 사용하는 단어를 패스워드로 선택하는 경우가 많으므로 패스워드의 추측이 용이한 경우가 많다. 패스워드의 추측을 어렵게 하려면 사용자가 보다 무작위하게 선택하거나 자동으로 시스템에서 패스워드를 무작위하게 골라주는 방법이 있다.

다. 패스워드 시스템 설계시 고려요소

패스워드 시스템을 설계, 구현 그리고 사용할 때에 고려할 요소는 여러가지가 있다. 이 절에서 설명하는 10가지 요소는 미국 FIPS(Federal Information Processing Standards)를 따른 것으로 보안 관리자의 판단에 따라 첨가 또는 삭제할 수 있는 것이다[8]. 패스워드 시스템을 운영할 때에 중요한 문제는 표준 준수 규정을 만드는 것으로 시스템 운영자나 보안 관리자가 보호하는 시스템 또는 자료의 보안 수준에 맞추어 결정한다.

(1) 패스워드의 구성 기능 문자 :

패스워드에 사용될 수 있는 유효한 문자를 구성가능문자라 한다.

(2) 패스워드의 길이 :

유효한 패스워드가 되기위한 패스워드의 길이 제한을 규정하는 것으로 최소값과 최대값 (예를 들면 6~8)을 정한다.

(3) 패스워드의 수명 :

하나의 패스워드가 이용될 수 있는 최대 기간(수명)을 말한다.

(4) 패스워드의 출처 :

패스워드를 만들거나 고를 수 있는 개체를 말하며 사용자, 보안 관리자 또는 자동 패스워드 생성기가 있다.

(5) 패스워드의 소유 :

패스워드를 사용할 권한이 있는 개인이나 집단을

규정한다.

(6) 패스워드의 분배 :

새로운 패스워드를 생성했을 때 그것의 소유주나 패스워드 시스템 내의 필요한 모든 곳에 전달하는 방법들을 규정한다.

(7) 패스워드의 저장 :

유효한 패스워드를 그것의 수명 동안 저장하는 방법을 말한다.

(8) 패스워드의 입력 :

사용자가 시스템에 자신을 인증하거나 자료의 접근권한을 얻기위해 시스템에 패스워드를 입력하는 방법을 말한다.

(9) 패스워드의 전송 :

패스워드의 입력장소로부터 비교장소까지 전송하는 방법을 규정한다.

(10) 패스워드의 인증기간 :

인증기간이란 한번의 터미널 세션이나 데이타 접근시 초기인증 과정과 이어지는 재인증 과정사이의 최대기간을 말한다.

라. 사용자의 보안

현재 일반적으로 이용되는 패스워드 시스템은 사용자가 직접 패스워드를 고르고 변경할 수 있다. 이와같은 시스템에서는 사용자의 패스워드 사용방법은 그들이 이용하는 시스템과 자료의 보안에 큰 영향을 끼친다.

(1) 보안에 대한 인식 :

사용자들은 패스워드 시스템을 스스로가 보호해야 한다는 의무감을 가져야 한다. 의심이 가는 보안위반이 있을 때나 입출력 장치의 동작에 변화가 있을 때는 보고를 하는 자세가 필요하다. 그리고 각 개인은 자신의 패스워드를 잊거나 타인에게 노출시키지 않도록 하여 비밀을 유지시켜야 한다.

(2) 패스워드의 기억 :

사용자는 자동 자료처리 시스템에 자신을 인증할 때마다 패스워드를 입력해야 하므로 자신의 패스워드를 꼭 알고 있어야 한다. 패스워드를 어떤 매개체에 적어놓고 볼 수도 있지만 분실의 위험이 있으며 그 매개체에 대한 보안이 또한 필요하게 되므로 반드시 기억해야 한다.

(3) 패스워드의 추측 가능성 :

패스워드를 사용자가 골라서 이용할 때는 그것의 추측이 어렵게 만들어야 한다. 보통 사용자들은 기억의 편의를 위해 자신과 관련된 전화번호, 주민등록번호, 주소, 주변인물 이름이나 생일, 특징 또는 자신의 과거 등을 이용하여 패스워드를 고르는 경우가 많다. 그러한 패스워드는 만약 시스템의 불법 침입자가 어떤 사용자에 대한 정보를 많이 가지고 있다면 쉽게 추측이 가능하므로 매우 위험하다. 따라서 사용자들은 무작위에 가깝게 패스워드를 고르도록 해야 한다.

(4) 패스워드의 변경 :

패스워드가 노출되었을 가능성이 있을 때 가장 쉬운 해결책은 패스워드를 바꾸는 것이다. 따라서 발견되지 않은 패스워드 노출의 가능성을 줄이기 위해서는 패스워드를 자주 교체해야 한다. 보안관리자가 패스워드의 수명을 제한하여 일정기간이 지나면 의무적으로 패스워드를 교체하도록 할 수도 있지만 사용자도 또한 패스워드 노출의 위험이 있을 때는 즉시 패스워드를 교체해야 한다.

(5) 패스워드의 입력 :

패스워드를 시스템에 입력할 때 보안을 유지하는 것은 어렵지 않으면서도 주의해야 할 사항이다. 전형적인 입력장치인 키보드를 이용할 때는 타이핑을 빨리, 여러 손가락을 이용하고 그리고 관찰자로부터 몸을 가리며 패스워드 입력을 해야 한다. 만약 주위에 관찰자가 있으면 패스워드의 일부 혹은 전부가 노출될 수도 있으므로 비켜달라고 요구할 수도 있고 주위사람들이 시스템 사용을 알기전에 패스워드 입력을 끝낼 수 있다.

(6) 패스워드의 발생 및 분배 :

시스템에 처음 가입할 때 사용자는 자신의 식별자만을 갖고 패스워드는 자신이 만들도록 요구받을

경우가 있다. 이때 패스워드를 만들지 않고 시스템을 사용하게 되면 누구든지 침입이 가능하게 되므로 반드시 패스워드를 만들어야 하며 빨리 만들수록 좋다. 만약 식별자와 함께 패스워드를 받았을 경우에는 그 패스워드를 이용하여 시스템에 들어간 후 빨리 자신이 선택한 패스워드로 교체해야 한다.

마. 관리자의 보안

보안 관리자는 시스템 전체의 보안에 책임이 있는 자로서 보호해야 할 시스템이나 자료에 따라 보안 수준을 결정한다. 그는 보안이 이루어지지 않았을 때 입는 손실과 보안에 필요한 경비를 비교 평가하여 보안 수준을 결정한다.

(1) 패스워드의 구성가능문자 :

패스워드는 95개의 그래픽 문자들 중 시스템 운영자와 보안 관리자가 정한 문자들을 이용하여 구성한다. 생성 가능한 패스워드의 수는 시행착오 공격으로 알아낼 수 없을만큼 커야하며 생성이나 선택이 쉽고 기억될 수 있어야 하며 저장이 가능하고 쉽게 입력될 수 있어야 한다. 패스워드의 구성가능문자는 입력장치, 저장방법 그리고 입력된 패스워드와 저장된 패스워드를 비교하는 방법과 연관이 있다.

구성가능문자의 최소값은 10이며 금융기관에서 이용하는 PIN(Personal Identification Number)이 10개의 문자(0~9)로써 구성된다[1]. 좀 더 나은 구성으로는 10개의 숫자에 A, B, C, D, E, F를 포함하여 패스워드를 16진수로 표현하는 것이다. 16진수 문자는 하나에 4비트 씩으로써 DES의 키이를 나타낼 때 이용한다.

많은 패스워드들은 영어 소문자(a~z)나 대문자(A~Z) 만을 이용하여 구성된다. 그러나 영어 알파벳으로만 이루어진 패스워드는 흔히 알고있는 영어단어를 이용하는 경우가 많으므로 안전하지 못하다. 따라서 영어 알파벳에 숫자를 넣는 방법이 좋으며 더욱 좋은 방법은 구성가능 문자로서 95개의 그래픽 문자를 이용하는 것이다. 자동 패스워드 시스템은 패스워드가 생성 또는 변경될 때 패스워드가 구성 가능 문자들로만 구성되었는지 검사할 수 있는 기능이 있어야 한다.

(2) 패스워드의 길이 :

패스워드의 길이는 시스템 운영자와 보안 관리자에 의해 선택된다. 패스워드의 길이는 최소 4문자 이상이어야 하며 10,000개 이상의 패스워드를 만들 수 있는 길이와 구성 가능 문자를 가져야 한다. 선택된 패스워드의 길이 범위는 보호하는 자료의 가치 또는 민감성에 비례하는 보안 수준을 제공해야 한다. 패스워드의 길이는 구성가능문자와 더불어 시행착오 공격에 대한 패스워드 시스템의 보안을 평가하는 기준이 된다. 예를 들어 은행의 PIN은 10개의 구성가능문자(0~9)를 가지고 길이가 4 이므로 10,000개의 패스워드를 만들 수 있다. 은행용 PIN 처럼 구성 가능 문자의 수가 작고 길이가 짧으면 추측이 보다 쉽지만 입력시 속도가 빠르고 정확히 기억할 수 있는 장점이 있다.

만약, 다른 모든 요소를 무시할 수 있다면 패스워드에 의한 보안은 길이에 비례하므로 패스워드가 길면 더 안전하다. 그러나 패스워드가 길수록 기억하기가 힘들고 입력시간이 길어져 보안의 위협요소가 될 수도 있다. 따라서 DES에 이용하는 64비트(16개의 16진수 문자로 나타냄)의 키이는 흔히 사용하지는 않는다.

암호구(passphrase)를 이용하면 패스워드보다 더 효과적으로 보안을 유지할 수 있다. 암호구란 이해할 수 있는 단어들의 모임으로서 문장이라고 쉽게 생각할 있다. 암호구는 실제로 자동자료처리 시스템에 저장되거나 그들 사이에서 통신될 때는 64비트의 가상 패스워드로 압축 변환된다. 가상 패스워드는 암호구가 입력이 되어 암호구가 조금 변하면 다른 값이 나오는 성질을 가져야 하며 64비트로 이루어지므로 최대 2의 64승 개의 패스워드를 만들 수 있다. 암호구는 쉽게 기억할 수 있는 잇점이 있지만 입력시간이 길어지는 단점이 있다.

(3) 암호 알고리즘의 공개여부 :

일방함수로서 사용되는 암호 알고리즘은 일반적으로 공개적으로 알려진 DES나 그것을 변형한 방식을 이용하는 수가 많다. 그러나 국가나 기관에서

독자적인 알고리즘을 개발하여 알고리즘을 공개하지 않고 이용할 수도 있다.

공개된 연구결과에 따르면 패스워드 시스템은 근본적으로 모든 알고리즘과 하드웨어가 공개되어도 패스워드의 비밀을 유지함으로써 전체 시스템의 보안을 유지해야 하므로 암호 알고리즘은 비밀을 유지할 수도 없고 또한 비밀로 유지할 필요도 없다고 학자들은 결론짓고 있다[5]. 그러나 보다 강도있는 보안이 필요한 특수 시스템에서는 하드웨어와 더불어 알고리즘의 비밀을 지키는 것이 효과가 있을 것이라고 본다.

(4) 패스워드의 수명 :

패스워드의 수명은 교체에 드는 비용, 노출되었을 때의 위험, 분배시의 위험, 추측할 수 있는 확률, 사용하는 횟수, 시행착오로 찾아낼 확률 등의 요인으로 결정한다. 만약 소유자나 보안 관리자에게 들키지 않고 패스워드가 노출되는 경우가 있더라도 패스워드를 다른 것으로 대체한다면 위험은 사라지게 된다. 따라서 패스워드는 주기적으로 바꾸어야 하며 노출되었다고 의심이 가거나 확신이 설 때에는 즉시 바꾸어야 한다. 패스워드 시스템은 사용자나 보안 관리자가 패스워드를 교체할 수 있도록 해야 한다.

패스워드 시스템은 자동적으로 수명이 다한 패스워드를 교체하게 하는 기능이 있어야 하며 새로운 패스워드가 기존의 것과 다른 것인지 비교하여 다를 때에만 받아들이게 해야 한다. 중요한 시스템은 과거의 N개까지 비교하는 수도 있다. 그러나 각 사용자들끼리 패스워드가 달라야 한다는 조건이 있어서는 안된다. 왜냐하면 만일 패스워드를 입력했을 때 시스템에 의해 거절당한다면 다른 사용자가 그 패스워드를 소유한다는 것을 알 수 있기 때문이다.

패스워드의 최대 수명은 1년 이하이어야 하며 원하는 수준의 보안을 유지하면서 가장 비용이 적게드는 방향으로 수명을 결정한다. 만약 사용자가 시스템 사용권한이 없어지거나 자료접근 권한이 없어질 경우는 적어도 3일안에 패스워드를 지우든지 유효하지 않은 패스워드로 교체해야 한다. 자동화된 패스워드 시스템은 보안 관리자가 자신을 인증한 후 사용자의 패스워드를 지우거나 교체할 수 있게 허락해야 하며 패스워드를 새로 만들거나 교체했을 때의 기록을 가져야 한다.

(5) 패스워드의 입력 :

컴퓨터 터미널이나, 키이보드, 푸쉬버튼, 또는 다른 패스워드 입력장치에 패스워드를 입력할 때는 노출을 최소화하도록 해야 한다. 패스워드를 터미널에서 입력할 때는 화면에 인쇄 되어서는 안된다. 천공카드를 이용하여 배치 프로세싱(batch processing)할 때에는 시스템에서 패스워드의 요구가 있을 때에 패스워드 카드를 천공카드의 제일 윗장에 포함해야 한다. 패스워드는 출력 미디어에 인쇄되어서는 안되며 처리가 끝난 후에는 패스워드 카드를 안전한 곳으로 옮기거나 파기해야 된다. 순서적으로 이용되는 패스워드의 목록이 이용될 경우에는 목록을 소유자가 물리적으로 보호해야 한다.

사용자가 패스워드를 입력할 때에는 한번 이상 3번정도 재시도 할 수 있는 기회가 주어져야 한다. 그러나 패스워드 입력을 재시도 할 때는 몇 초 혹은 몇 분 간격을 두어 자동화되고 속도가 빠른 시행착오공격을 막아야 한다.

패스워드 시스템은 사용자가 로그인을 성공했을 때 바로 그전의 로그인 성공과의 사이에 있었던 실패한 패스워드 입력시도에 대한 메시지를 보내 사용자의 패스워드에 대한 공격이 있었음을 알려야 한다. 부정한 패스워드 입력시도의 횟수가 최대한도를 넘을 때에는 경보를 울려 보안 관리자가 조치를 취할 수 있어야 한다.

(6) 패스워드의 소유 :

자료에 대한 접근 패스워드는 여러 사람이 공유할 수 있지만 개인 패스워드는 반드시 개인적으로 가져야 한다. 그 이유는 개인 패스워드가 달라야만 누가 무슨 자료에 어떤 목적으로 접근하였나를 결정할 때 개인의 책임을 알 수 있으며 패스워드의 불법 사용이나 분실을 알 수 있기 때문이다. 또 사용자의 시스템 사용활동에 대한 감사를 개인적으로 할 수 있으며 단체의 한 구성원이 떠나거나

시스템 사용권한을 잃었을 때 단체 구성원 모두가 패스워드를 바꿀 필요가 없기 때문이다.

접근 패스워드는 자료를 만든 그 개인만이 소유하거나 자료에 접근 권한이 있는 개인들만이 가질 수 있다. 한 개인이 가진 패스워드와 그가 권한이 있는 자료의 접근 패스워드는 의도적으로 선택되거나 같아서는 안된다.

(7) 패스워드의 발생과 출처 :

패스워드의 출처는 보안 관리자와 시스템 운영자가 선택하며 사용자, 보안관리자 또는 자동 패스워드 발생기중의 하나 혹은 여럿이 될 수 있다. 흔히 보안 관리자는 시스템의 신규 사용자를 위해 패스워드를 선택한다. 그 패스워드는 정해져 있거나 사용자의 식별자와 관련되서는 안되며 무작위해야 한다. 사용자는 그것을 이용하여 시스템에 들어간 후 패스워드를 바꾼다. 새로 선택된 개인 패스워드는 자동 패스워드 시스템에 의해 정해진 표준에 맞는지 검사되며 표준에 맞지 않으면 거부된다. 패스워드를 시스템이 만들 때에는 생성방법이 추측 가능하면 안되며 보통 무작위 숫자 발생기를 이용한다.

새 시스템에는 시스템 운영자, 시스템 프로그래머와 보안 관리자를 위한 패스워드가 전달되고 설치된다. 그 패스워드들은 보안 관리자에 의해 시스템에서 유효하지 않거나 새로운 무작위한 패스워드로 바꾸거나 권한이 있는 사용자가 소유하는 유효 패스워드로 즉시 바꾸어야 한다.

(8) 패스워드 화일의 저장 :

인증 시스템에서 패스워드를 저장할 때는 패스워드가 노출되거나 권한이 없는 사람이 교체할 수 없어야 하며 오직 로그인 프로그램에 의해서만 패스워드 화일을 읽고 쓸 수 있어야 한다. 즉 저장된 패스워드는 패스워드 시스템만이 접근 권한이 있어야 한다. 패스워드의 교체 역시 권한이 있는 보안 관리자나 정당한 절차로 자신을 인증한 사용자에 의해서만 가능하다.

패스워드 화일의 보호는 시스템의 보안이 요구하는 수준에 따른다. 그 수준에 따라 패스워드 화일은 저장할 때에 암호화할 수도 안 할 수도 있으며 화일에 대한 접근권한 역시 일반사용자에게 줄 수도 주지 않을 수도 있다.

패스워드 화일을 암호화할 때는 자료 암호화 키이를 이용하여 일방적 또는 양방적으로 할 수 있다. 이 때 자료 암호화 키이는 키이 암호화 키이에 의해 암호화되어 보호되어야 한다. 양방적 암호 시스템은 입력된 패스워드를 암호화하여 저장된 패스워드와 비교할 수도 있고 저장된 것을 복호화하여 비교하는 방식을 쓸 수도 있다. 일방적 암호 시스템은 패스워드를 암호화하면 다시 원래의 패스워드로 복원할 수 없으므로 사용자가 시스템에 로그인할 때에 입력된 패스워드를 암호화하여 저장된 것과 비교하는 방법을 이용한다.

(9) 패스워드의 분배 :

개인 패스워드는 출처로부터 만들어진 후 소유자 한 사람만 볼 수 있도록 분배되어야 한다. 패스워드가 사용자에 의해 선택되었을 때는 사용자로부터 인증 시스템에 전달되어야 하며 패스워드 시스템에 의해 생성되었을 때는 사용자에게 전해져야 한다. 또 보안 관리자에 의해 만들어졌을 때는 사용자와 인증 시스템에 전달 되어야 한다.

초기 패스워드는 패스워드 교체 때와는 다른방식으로 분배된다. 초기 패스워드는 일반적으로 말로 혹은 등기편지로써 시스템 사용권한이 있거나 자료접근 권한이 있는 사용자에게 전달된다. 이것은 한번 쓰고 버리는 패스워드로 시스템에 일단 들어간 후 반드시 사용자에 의해 교체되어야 한다.

패스워드는 출처로부터 분배될 때 임시저장장치에 남겨져서는 안되며 패스워드를 오랜 시간동안 가질 수 있는것은 오직 사용자와 패스워드 시스템 뿐이어야 한다. 패스워드의 교체는 사용자가 기존의 패스워드로 자신을 확인시키고 새로운 패스워드를 입력함으로써 수행된다. 교체시에는 패스워드가 보안표준에 맞는지 검사하고 기존의 패스워드와 같은지 검사하여 다르면 그 위치에 저장된다.

패스워드를 편지로 분배할 때는 반드시 봉함한 봉투에 넣어 분배해야 한다. 사용자의 주의사항으로는 1) 쓰여진 패스워드를 암기한 후 없앤다. 또는 2) 패스워드를 수취했음을 서명하고 봉투에 봉함한

후 보안 관리자에게 다시 보낸다. 3) 패스워드를 가능한 빨리 사용하고 만약 사용자가 바꿀 수 있으면 패스워드를 교체한다.

어떤 시스템은 패스워드를 컴퓨터로 인쇄하여 편지에 봉함하여 분배한다. 우편물은 일단 개봉하면 다시 원래대로 봉함할 수 없는 것을 이용한다. 우편물 안은 윗장에 수신자의 이름이 쓰여있고 그것을 뜯으면 그 안에 패스워드가 있다. 그래서 윗장이 뜯어진 후 뒷장만을 누가 가지게 되도 누구의 것인지 알 수 없게 하는 것이다.

패스워드를 안전한 우편물을 이용하여 분배하고 수신을 확인했을 경우 기존의 패스워드와 새 패스워드가 바뀌는 과정에서 과도기간이 있을 수도 있다. 어떤 시스템은 그 기간동안 두가지를 다 유효하게 허용하기도 하고 과도기간을 허용하지 않고 정확한 시간에 패스워드를 교체하는 수도 있다.

패스워드가 분배 될 때에 생성 또는 변경된 날자, 시간등의 감사 기록을 남겨 보안 관리자가 이를 감사용으로 이용할 수 있어야 한다. 자동 패스워드 시스템은 패스워드 생성과 분배시 생성 날자와 시간과 누구에게 분배되었는지를 자동으로 기록하며 패스워드 교체시에도 기록을 남긴다.

(10) 감사 기록 :

감사 기록이란 보안 관리자가 알 수 있도록 패스워드 시스템에 사용자들의 패스워드 이용 행적을 기록하는 것을 말한다. 즉 패스워드를 처음 만든 시기, 교체한 시기, 입력 실수의 시기 및 횟수 등을 기록한다. 패스워드의 입력이 잘못된 경우가 어느 한도 이상 많아지면 그것은 불법적인 입력시도가 있었음을 알려주는 지표가 될 수 있다. 또한 한번에 몇 번 이상 올바른 패스워드를 입력하지 못했을 때는 보안 관리자가 즉시 체크 할 수 있도록 벨을 울리거나 이상 신호를 발생한다. 감사 기록은 수시로 보안 관리자가 검사하여야 하며 보안 수준에 맞추어 종목을 결정할 수 있다. 예를 들면 1) 어떤 사용자의 패스워드 입력 실수가 허용횟수를 넘었을 때 2) 한 터미널에서 입력 재시도가 허용횟수를 초과했을 때 3) 정해진 기간안에 허용횟수보다 많은 입력시도가 있을 때(이는 자동화된 시행착오 공격을 막기위함) 보안 경보가 울릴 수 있다. 이와 같은 조건은 보호하는 시스템과 자료의 중요성에 맞추어 결정한다. 만약 경보가 울리면 터미널은 동작 불능이 되고 서비스는 거부되어야 하며 오직 보안 관리자 만이 터미널을 재동작 시키고 다시 서비스를 받을 수 있게하는 권한이 있다.

(11) 패스워드의 인증기간 :

개인 패스워드는 사용자가 시스템에 로그인 할 때마다 인증하며 접근 패스워드는 보호하는 자료에 처음 접근할 때에 인증되어야 한다. 원격 터미널을 통한 사용자와 시스템간의 통신은 종종 오랜 시간이 걸리곤 한다. 이때 사용자가 터미널의 자리를 비워두는 상황이 생길 수 있다. 그러한 경우는 만약 패스워드 시스템 사용기관 내부에서 어떤 불순한 목적을 가진 사람이 있을 때에는 매우 위험하다. 실제로 은행등 금융기관에서는 잠깐 자리를 비운 터미널을 이용한 컴퓨터 범죄행위가 자주 있다. 그래서 많은 시스템들은 터미널의 활동이 한동안 없으면 자동적으로 로그아웃 시키기도 한다.

어떤 접근 제어 시스템은 초기 인증외에도 주기적으로 재인증을 요구하기도 한다. 이러한 시스템은 인증 빈도가 많을 경우 사용자들이 싫어하는 수가 있으므로 매우 보안수준이 높은 때에만 이용된다. 이러한 경우도 중요한 작업을 하고 있는 중간에 인증 과정이 일어나면 곤란하므로 터미널이 어느 기간만큼 활동이 없을 때에만 재인증을 요구해야 한다.

(12) 패스워드의 전송 :

패스워드는 전형적으로 컴퓨터 네트워크나 시분할 원격 접근 컴퓨터 시스템에서 접근 권한을 얻기위해 자신을 인증하는 과정에 사용한다. 따라서 인증을 하기 위해서는 터미널과 컴퓨터 사이의 통신선을 따라 패스워드를 전송해야 한다. 만약 통신선이 물리적으로 보안이 이루어지지 않았다거나 전송되는 패스워드가 암호화되지 않았다면 통신되는 패스워드는 노출위험이 클 것이다. 현재의 대부분의 통신선은 그러한 보안이 이루어지지 않은 상태이므로 사용자들은 자신의 패스워드가 수동적 라인 태핑을 이용하면 쉽게 노출 될 수 있음을 알아야

한다. 수동적 라이태핑이란 통신 내용을 도청하는 것으로 값싼 기본적인 기술만으로도 쉽게 할 수 있다.

적극적 라인태핑이란 통신내용을 중간에서 가로채 내용을 변경하여 다시 전송하는 것을 말한다. 이와 같은 장비는 비싸지 않은 가격에 구입되어 PC에 연결되어 사용될 수 있다. 적극적 라인태핑을 이용하면 통신되는 패스워드를 다른 것으로 대치할 수도 있으며 터미널의 사용자와 컴퓨터를 모두 속여 패스워드를 알아낼 수도 있다. 그 과정을 설명하면 중간에 다른 컴퓨터가 있음에도 불구하고 터미널 사용자는 자신이 원하는 컴퓨터와 연결되어 있다고 믿고 컴퓨터 또한 올바른 사용자와 연결되었다고 믿는다. 그래서 터미널에서 로그인 과정을 동작시키고 패스워드를 입력하면 중간의 침입자는 패스워드만 알아낸 후 컴퓨터가 현재 일시적으로 동작불능이라고 터미널 사용자에게 알린다. 이 과정에서 침입자는 사용자가 전혀 모르게 그의 패스워드를 알아낼 수 있다.

이와같은 위험은 암호를 이용하여 두가지 방법으로 해결할 수 있다. 첫번째 방법은 터미널과 컴퓨터에 암호장비를 추가하여 양자간의 모든 통신내용을 암호화하는 것이다. 그러면 중간에서 통신내용을 엿듣는다 해도 패스워드를 알아낼 수 없다. 게다가 각 전송때 마다 숫자를 넣어 암호화시키면 통신 내용을 저장하여 다시 사용하는 경우를 막을 수 있다.

두번째 방법으로 패스워드를 암호 키이로 이용할 수 있다. 사용자가 패스워드를 입력하면 그것을 암호 키이로 작용하여 터미널과 컴퓨터 사이의 통신내용을 보호한다. 컴퓨터는 사용자의 키이를 가지고 있으므로 암호화된 통신 내용을 다시 복호화 할 수 있다. 이 과정은 통신선을 따라 사용자의 키이 자체는 전달되지 않는 특징이 있다.

패스워드가 입력 장소에서 비교 장소까지 전송될 때에는 그것이 보호하는 시스템이나 자료만큼은 패스워드를 보호해야 하며 그 수준은 보안 관리자가 결정한다.

3. 결 론

패스워드의 사용은 컴퓨터 보안에 있어서 일부에 지나지 않는다. 하지만 대부분의 컴퓨터 시스템이 패스워드를 이용해서 사용자를 인증하고 자료에 대해 접근을 제어하고 있으므로 그에 따라 패스워드의 사용법은 아주 중요한 문제라 할 수 있다. 패스워드는 컴퓨터 네트워크나 시분할 원격접근 컴퓨터 시스템에서 주로 사용하므로 시스템에 침투하고자 하는 자는 컴퓨터와 멀리 떨어진 곳에서 직접적인 위협을 느끼지 않고도 침투 시도가 가능하다는 특징이 있다. 실제로 해커에 의한 시스템 침투 사례는 여러가지가 알려져 있다.

정보화시대로 가고있는 현 시점에서 그와같은 시스템의 보안위협은 커다란 자산의 손실 또는 사회적 혼란을 초래할 수 있다. 본고에서는 패스워드를 이용하는 컴퓨터 시스템에서 일어날 수 있는 여러가지 문제점을 살펴보고 그에 대한 대책을 논의하였다. 컴퓨터 보안에는 여러 기술적, 법적, 교육적, 물리적, 행정적인 대책들이 또한 필요하나 이 글에서는 패스워드시스템 사용에 있어서의 기술적인 대책방안과 사용자와 관리자가 지켜야 할 규범사항들에 대한 논의로 그 범위를 제한하였다.

참 고 문 헌

1. D.W. Davis & W.L. Price, *Security for Computer Networks*, John Wiley & Sons, 2nd Ed., p.169, 1989

2. Arthur Evans, Jr., William Kantrowitz & Edwin Weiss"A User Authentication Scheme Not Requiring Secrecy in the Computer" *Comm. ACM* Vol.17, No. 8, pp.437-442, 8/74

3. *Data Encryption Standard*, FIPS PUB 46, 1977

4. 한국 표준 KS C5766-1986, 데이타 보호 알고리즘 (DEA1) 명세

5. David C. Feldmeier and Philip R. Karn "UNIX Password Security-Ten years Later" In *Proceeding of Crypto'89*, August 1989

6. Robert Morris and Ken Thompson "Password Security : A Casc History" *Comm. ACM* Vol.22, No.11, pp.594-597, 11/79

7. R.C. Summers "An overview of computer security" *IBM System Journal*, Vol.23, No.4, 1984

8. *PASSWORD USAGE*, FIPS PUB 112, 1985

□ 著者紹介

李 弼 中(正會員)

1951年 12月 30日生
1974年 2月 서울大學校 電子工學科 學士
1977年 2月 서울大學校 電子工學科 碩士
1982年 6月 U.C.L.A. System Science, Engineer
1985年 6月 U.C.L.A. Electrical Engineering, Ph.D.
1980年 6月～1985年 8月 : Jet Propulsion Laboratory, Senior Engineer
1985年 8月～1990年 2月 : Bell Communications Research, M.T.S.
1990年 2月～現在 : 浦港工科大學 電子電氣工學科, 副教授

文 熙 哲(正會員)

1968年 5月 9日生
1990年 2月 韓國科學技術大學 情報通信科 學士
1990年 3月～現在 : 浦港工科大學 電子電氣工學科, 碩士過程 在學中