대규모 조직에서의 패스워드 관리에 관한 권고 고찰

박 진 섭*

목 차

Ⅰ. 서론

본고의 목적은 문자위주의 패스워드에 대한 공통적 위협을 분석하고 이와 같은 위협을 어떻게 각 조직이 경감시킬 것인가를 제시한다. 언급한 주제는 패스워드정책 요구사항 정의하기, 중앙 집중식, 로컬 패스워드 관리 솔루션을 포함한다. 비문자형 패스워드(그래픽 기반 패스워드 등)는 제외한다.

길고 복잡한 패스워드는 공격자가 추측이나 크래킹을 힘들게 하지만, 사용자가 패스워드를 기억하기 힘들게 하고, 오히려 메모 해두는 방법

* 대전대학교 컴퓨터공학과 교수

등으로 보안을 더 약하게 하여 공격자에게 위험을 노출시키기도 한다.

각 조직은 패스워드 기반 인증을 사용에 따른 약점을 인식해야만 한다. 패스워드에는 여러 가지 위협이 있으며, 이들 위협의 대부분은 부분적으로 경감 시킬 수 있다. 또한 사용자는 많은 패스워드를 관리해야 하고 기억해야하는 부담을 갖게 된다.

그러나 조직 패스워드 관리 메커니즘이 이와 같은 부담을 경감시킨다 해도 사용자는 사용상 단점을 가지며, 심각한 보안 사고를 발생 시킬 수 있다.

왜냐하면 단일 인증자를 통하여 여러 시스템에 접근을 허용할 수 있기 때문이다. 그러므로 각 조직은 좀 더 강력한 형태의 패스워드 기반 인증으로 대체하거나 보완할 장기 계획을 수립해야한다. 각 조직들은 각자의 패스워드 기밀을 보호하기위해서 다음과 같은 권고들을 수용할 필요가 있다.

1. 범 조직적인 패스워드 관련 요구사항을 명시한 패스워드 정책의 수립

패스워드 관리와 관련한 요구사항들은 패스워드 저장, 전송, 패스워드 구성 그리고 패스워드 발급과 초기화 절차들을 포함하고 있다. 여기에서 언급하는 권고에 추가하여 각 조직들은 계정 적용 법령과 패스워드와 관련한 다른 가이드라인과 요구사항들을 수용해야한다. 어떤 조직의 패스워드 정책은 여러 운영체제와 어플리케이션에 의해 제공되는 다양한 패스워드 관련 기능을 수용 할 수 있는 유연성을 제공해야 한다. 예를 들면 암호 알고리즘과 패스워드 문자 집합이 다르게 제공되고 있다. 조직들은 패스워드 관리와 관련한 주요 기술변화가 발생 할 때 정기적, 부분적으로 패스워드 정책을 재검토해야 한다.

2. 패스워드 탈취 공격으로부터의 패스워드 보호

공격자들은 여러 가지 방법으로 패스워드를 탈취한다. 예를 들면 공격자들은 호스트에 저장된 OS와 어플리케이션 패스워드에 접근하기위한 시도를 한다. 그와 같은 패스워드는 패스워드 암호 해쉬 방법 등으로 저장한 파일을 접근을 제약하는 것과 같은 부가적인 보안통제를 사용하여 저장된다. 네트워크를 통하여 전달하는 패스워드는 패스워드 암호화 같은 방법으로 스니핑 위협으로부터 보호해야한다. 사용자는 피싱 공격, 키보드 자판 로거, 훔쳐보기와 같은 행위에 대한 인식을 해야 하며, 그와 같은 공격이 발생 할 때 어떻게 대응해야하는가를 알고 있어야한다.

각 조직들은 패스워드를 잊은 경우와 패스워드를 초기화 하려는 사용자를 식별하고 검증 할 필요가 있으며, 이를 통하여 패스워드가 공격자에게 실수로 노출되지 않도록 해야 한다.

3. 패스워드 추측과 크래킹 가능성 감소를 위한 패스워드 메커니즘의 구성

패스워드 추측 공격은 보다 쉽게 완화 시킬 수 있다. 즉 패스워드를 보다 복잡하게 만들고, 연속적인 인증시도 실패 시 인증시도를 제한시킴으로서 가능하다.

패스워드 크래킹 공격은 강력한 패스워드의 사용, 강력한 암호 알고리즘을 통한 패스워드 해시 구현, 패스워드 해시의 기밀보호 등으로 완화 시킬 수 있다.

또한 정기적인 패스워드 변경은 보다 쉽게 크래킹 등에 의한 위험을 감소시킬 수 있다.

패스워드 강도는 패스워드의 복잡성, 패스워드 길이, 사용자의 패스워드 지식 등 여러 가지 요소에 의존한다. 각 조직들은 패스워드 강도에 대한 정책 요구사항을 수립할 때 이런 요소를 고려해야하며, 패스워드를 기억 할 필요가 있는 사용자인지 여부 등을 포함해야 한다.

4. 보안 필요성과 사용성과의 균형을 기초로 한 패스워드 실효만기를 위한 요구사항의 결정

많은 조직들은 패스워드 월권 사용의 잠재적 영향을 감소시키기 위해서 패스워드 실효만기 메커니즘을 실시하고 있다. 이것은 어떤 경우에는 유익한 반면에 공격자가 과거 패스워드를 탈취하기위해 사용했던 과 같은 키보드 로거를 통하여 신규 패스워드를 위태롭게 할 수 있는 비효율적인 측면이 있다.

패스워드 실효만기는 사용자 불만의 원천이 되고 있다. 즉 사용자는 수심개의 계정에 대하여 수개월 마다 신규 패스워드를 생성하고 기억하게 하며, 이것은 여러 계정에 같은 패스워드를 적용하게 하며 단순 패스워드를 선택하게 만든다. 각 조직들은 패스워드 실효 만기 요구사항을 결정 할 때 여러 가지 요소를 고려해야한다. 즉 사용자 패스워드의 안전한 저장장치 가용성, 패스워드에 대한 위협 수준, 인증의 빈도(일일 단위/년 단위), 패스워드 저장장치의 강도, 크래킹에 대한 패스워드 실효만기의 효과성과 비 효과성 등을 포함해야 한다. 각 조직들은 자신의 보안 필요성과 편의성 요구사항은 반영하여 OS와 어플리케이션 등을 포함한 다양한 형태의 시스템에 대한 패스워드 실효만기에 대한 각기 다른 패스워드 정책을 고려해야한다.

본고는 미국 국립기술표준원(NIST)에서 미국 연방정부 기관에 권고하고 있는 패스워드 관리에 관한 특별기술 권고문서 800-118을 중심으로 기술한다.

Ⅱ. 패스워드 관리 개요

패스워드는 사용자가 자신임을 인증하는 핵심요소(일반적으로 문자열)이다.

개인의 이름과 같이 사용 식별자를 가진 패스워드 사용은 신원식별과 인증의 한 형태이다. 신원식별이란 시스템에서 사용자를 식별하도록 요구자를 구분하는 것이다. 인증은 요구자에 대한 검증으로 정보시스템에서 자원에 대한 접근을 승인하기위해 신뢰를 확보하는 과정이다.

인증은 사용자가 알고 있는 것(예 : 패스워드), 사용자가 소유하고 있는 것(예 : 스마트카드), 혹은 사용자 신체정보(예 : 지문, 음성패턴)를 포함할 수 있다.

패스워드만을 사용한 인증은 세 가지 인증 형식중의 하나일 뿐이며, 이중결합 인증은 세 가지 인증형식 중 두 가지를 사용하는 것이며, 삼중결합 인증은 위의 세 가지 요소를 모두 포함하는 것이다. 좀 더 부가적인 인자의 추가는 시스템에 대한 비승인 접근을 좀 더 어렵게 해준다. 예를 들면 사용자의 패스워드 와 스마트카드를 모두 도난당하는 경우보다 어떤 하나의 도난이나 누출이 훨씬 쉽기 때문이다.

여러 가지 보안형태에서 인증방법의 선택은 다양하지만, 패스워드는 가장 보편적인 방법으로 사용되고 있다.

패스워드는 데이터, 시스템, 네트워크를 보호하기위해 많은 곳에서 사용되고 있다. 예를 들면 패스워드는 운영체제, 어플리케이션(예 : 전자우편, 사번), 하드웨어, 원격접근 솔루션 등의 사용자를 인증하는데 사용되고 있다. 또한 패스워드는 파일과 패스워드로 보호되는 단일 압축파일, 암호 키, 암호화된 하드 드라이브 등과 같은 다른 저장정보를 보호하는데 사용되고 있다.

부가적으로 패스워드들은 가끔 비시각적인 방법으로 사용되기도 한다. 즉 생체인식장치는 지문스캔을 기반으로 하고, 홍채인식은 안구를

기반으로 패스워드를 생성 한다.

패스워드에는 다양한 형태가 있다. 그 하나는 잘 알려져 있는 PIN(personal identification number)이다. PIN은 상대적으로 짧고(보통 4~6 자), 단지 숫자로 구성된다. PIN 의 예는 "7352", "832290"이다. 다른 형태의 패스워드보다 입력하는 시간이 짧으며, 인명 안전 문제(화재 진압 시스템, 공조 타워 콘솔 등)와 관련해서는 좀 더 복잡하고 긴 형태로 사용되고 있다. 또한 PIN들은 경보 시스템, 자동판매기(ATM), 보안 토큰장치, 작은 키패드를 가진 기타 장치에 사용되고 있다. PIN들은 가끔 IT 시스템 접근을 위한 인증 형태로 사용되기도 한다. 본 서술에서는 PIN을 패스워드라는 용어 범주에 포함 한다.

패스워드의 특별한 다른 형태로는 관용구(passphrase)가 있다. 이것은 상대적으로 긴 연속적인 일련의 단어로 구성된 관용구나 하나의 문장과 같은 패스워드를 말한다. 관용구는 일련의 임의의 문자나 숫자, 특수문자(예 : "72*^dSd!", C8ke2.e3:")보다 기억하기가 보다 쉽고 단일 단어 패스워드보다 길이가 길다는 특성을 가진다.

그러나 "iloverocknroll"과 같은 단순한 패스프레이즈는 "9j%a#F.0"보다 공격자가 예측이 쉽다. 그리하여 관용구길이 자체만으로 다른 패스워드보다 강력하지는 않다고 볼 수 있다. 본 서술에서 패스워드 의미는 기존 패스워드와 관용구의 의미를 포함하는 것으로 본다.

패스워드관리란 범 조직 내에서 패스워드정책을 정의하고, 구현하고, 유지하는 과정이며, 효과적인 패스워드관리는 패스워드 기반 인증시스템을 위험으로부터 완화시킨다. 각 조직은 패스워드의 기밀성, 무결성, 가용성을 보호 할 필요가 있으며, 이는 모든 인증된 사용자(비인증 사용자 포함)가 필요시 성공적으로 패스워드를 사용 할 수 있게 해준다.

무결성과 가용성은 일반적인 데이터 보안 통제에 의해 보장 되어야한다. 패스워드의 기밀성을 보장 하기위해서는 좀 더 많은 보안 통제가 필요하다. 예를 들어 공격자가 패스워드를 추측하거나 크랙 할 수 없도

록 구성한 길고 복잡한 패스워드는 사용자가 기억하기가 힘들어 안전하지 않게 저장(메모 기록 등)하게 한다. 이것은 오히려 사용자의 패스워드를 불안전하게 하여 공격자에게 누출될 수 있다.

각 조직들은 사용자 이름과 같은 사용자 식별자에 대한 기밀성을 보호하는 것에 관심을 가져야 한다. 식별자를 기밀로 하는 것은 공격자가 목표로 하는 공격을 어렵게 할 수 있기 때문이다. 그러나 많은 경우에 식별자를 기밀로 하는 것은 도움이 되지 않는다. 왜냐하면 식별자는 사용자의 e-메일주소, 성명 등을 사용하기 때문에 공격자가 쉽게 파악하기 때문이다. 보다 보안이 필요한 상황, 즉 공격목표가 될 수 있는 상황에서는 조직과 관련한 식별자와 상이한 식별자 스킴을 사용하는 것이 유용 할 수도 있다. 만약 사용자가 여러 시스템에 걸쳐 같은 패스워드를 사용한다면 각기 다른 식별자를 사용하는 것은 사용자의 패스워드가 다른 시스템에서 재사용 된다고 할지라도 공격자에게 덜 노출될 수 있다. 그러나 서로 다른 식별자를 사용하는 것은 보안성에 제약을 가진다. 왜냐하면 그만큼 많은 위협들이 패스워드와 함께 식별자를 탈취하기 때문이며, 사용자는 식별자들을 기억하거나 기록해 두어야하기 때문이다.

조직은 패스워드관리와 관련한 모든 요구사항을 명시한 패스워드 정책을 가지고 있어야한다. 이 요구사항들에는 패스워드 저장장치, 전송, 패스워드 구성, 패스워드 발급과 초기화 절차 등을 포함해야한다. 또한 부가적으로 패스워드와 관련한 법/제도적 요구사항을 반영해야 한다. 각 조직의 패스워드 정책은 다양한 운영체제와 어플리케이션에서 제공하는 다양한 패스워드 관련 기능을 수용 할 수 있도록 유연성을 보유해야 한다. 암호 알고리즘과 패스워드 문자 집합은 다양하게 지원한다. 또한 정책들은 다른 패스워드 메커니즘에 의해 제공되는 보호를 수용해야 하며, 이들 메커니즘의 취약점을 명시 할 필요가 있다.

정책 개발이 완료된 이후에 각 조직은 패스워드정책을 구현 할 보안

통제를 선택해야한다. NIST SP 800-53은 식별과 인증과 관련한 많은 보안통제사항을 명시하고 있다.

미국 연방정부에서 권고하는 NIST SP 800-53에서 요구하는 통제들은 시스템의 보안 구분(FIPS Publication 199-low, moderate, or high.)을 기준으로 설정하고 있다.

조직은 패스워드관리에 영향을 미치는 주요 기술이 변경(신규 데스크 탑 운영체제)되는 경우에 정기적으로 혹은 부분적으로 패스워드 정책을 재검토해야 한다. 또한 조직은 패스워드 정책을 만족하는지를 보장하기 위해 패스워드와 관련한 보안 통제들을 재검토해야 한다.

패스워드와 패스워드 기반 인증 메커니즘을 안전하게 하는 것에 추가하여 각 조직들은 정기적으로 좀 더 강력한 인증으로 발전시키기 위한 평가를 해야 한다. 패스워드에는 여러 형태의 위협이 있으며, 이들 위협의 대부분은 부분적으로 완화 시킬 수 있다. 여기에서는 위협을 설명하고 가능한 완화 대책을 고찰한다. 사용자는 증가되는 많은 패스워드를 기억하고 관리하는 부담을 가진다. 조직의 패스워드 관리를 위한 현재 메커니즘들이 이러한 부담을 완화 시킬 수 있다 할지라도 사용상 불편을 초래하게 하고, 심각한 보안 사고를 야기 할 수 있다. 왜냐하면 단일 인증을 통하여 많은 시스템에 접근을 허용하기 때문이다. 그러므로 각 조직은 보다 향상된 보안요구를 가진 자원에 대한 인증을 강화하기위해 패스워드 기반 인증을 대체 할 장기 계획을 수립해야한다.

Ⅲ. 패스워드에 대한 위협과 완화

패스워드의 기밀성에 대한 위협은 네 가지 유형으로 구분한다.

1) 직접적인 패스워드 탈취 위협(키보드 로거의 설치)

2) 취약한 패스워드와 패스워드 해시의 편의성으로부터의 위협

(패스워드의 추측과 크래킹)
3) 패스워드 바꾸기 위협
4) 노출(손상)된 패스워드를 재사용 할 때의 공격자의 위협

이들 네 가지 위협 그룹들을 분석하고 이들 위협을 완화시키는 권고들을 서술한다.

1. 패스워드 탈취

탈취는 공격자가 저장장치, 전송 혹은 사용자에 관한 지식이나 행동 등을 통하여 패스워드를 취득하는 경우를 말한다. 여기에서는 이들 각 영역에 대한 공통적인 위협을 제시하고, 어떻게 완화 할 것인가에 대한 권고를 서술한다.

1) 저장장치

OS와 어플리케이션 패스워드가 인증에 사용되기 위해서는 호스트에 저장되어야한다. 만약 저장된 패스워드가 안전하지 않게 저장된다면 공격자는 물리적/논리적으로 호스트에 접근하여 패스워드를 얻을 수 있다. 패스워드가 보호되기 위해서는 별도의 보안 통제 없이 저장되어서는 안 되며, 보안통제의 예는 다음과 같다.

① 패스워드를 가진 파일을 암호화하기.

이것은 운영체제나 어플리케이션, 혹은 패스워드의 기밀성을 확보하기위해 특별히 설계된 패스워드관리 소프트웨어 같은 특별 유틸리티 등에 의해서 수행되어야한다.

② 패스워드를 포함하고 있는 파일에 접근을 제한하기 위해서 운영체

제 접근통제 특성을 사용하기.

호스트는 관리자에게만 허가되는 구성을 통하여 관리자 수준의 권한으로 이 실행을 하며, 사용자 수준으로 패스워드에 접근하는 것을 방지하는 것이다.

③ 패스워드 자체를 저장하는 대신에 패스워드에 대한 단방향 암호 해시 저장하기.

해시의 사용은 인증시스템이 실제 패스워드를 저장하지 않고 입력되는 패스워드가 정확한지를 검증할 수 있도록 해준다. 따라서 공격자는 해시에 대한 접근으로 대응되는 패스워드를 알 수가 없다.

특정 상황에 적합한 보안통제는 여러 가지 요소에 의해서 결정된다. 가령 호스트의 보안 역량, 호스트에 대한 위협들, 인증 요구사항 등이다. 예를 들면 암호 해시는 인증 프로토콜이 입력된 패스워드와 직접적으로 저장된 패스워드와 비교할 것을 요구한다면 필수 사항이 되어야 한다.

또한 해시에 대한 접근이 가능한 공격자가 패스워드의 생명주기내에서 패스워드를 크랙 했다면 운영체제 접근통제목록 같은 부가적인 통제로 해시에 대한 접근을 제한 할 필요가 있다.

공공기관들은 국가에서 승인한 암호 알고리즘을 사용하여 패스워드를 보호 해야만 한다. 많은 인증시스템은 승인된 암호 알고리즘만으로 패스워드를 보호 할 수 있도록 지원하고 있어 별도의 국가 승인이 필요 하지는 않다. 그렇기 때문에 공공기관들은 국가 승인 암호를 사용하여 패스워드 보호하기위한 통제를 보완하여 사용해야한다.

각 조직들은 어플리케이션에 의해 저장된 패스워드와 패스워드 해시를 어떻게 보호해야 하는지를 주의 깊게 고려해야한다. 예를 들면 웹 브라우저, E-메일 사용자, 기타 어플리케이션은 사용자의 편의대로 패

스워드를 저장 할 수 있다. 그러나 이것은 패스워드가 얼마나 안전한지 알 수 없다.

대부분의 경우에 이들 어플리케이션은 자동적으로 사용자의 식별을 검증하지 않고 필요한 만큼의 패스워드를 채운다. 사용자의 식별은 공격자에게 패스워드를 직접 사용 할 수 있도록 해준다.

패스워드관리 유틸리티는 사용자의 패스워드를 저장하는데 사용 될 수 있으나, 원하는 수준의 보안을 달성하기 위해서는 적절한 구성이 필요하다. 각 조직들은 어떤 어플리케이션이 사용자의 편리성과 그에 따른 위험을 고려하여 패스워드와 패스워드 해시를 저장 할 것인지를 결정해야 한다. 각 조직들은 자신의 패스워드 정책의 요구사항이 있어야 한다. 즉 어떤 어플리케이션은 패스워드와 해시가 어떻게 저장되어야 하는지를 고려해야한다.

호스트의 저장매체(예: 하드 드라이브)에 저장되는 경우에 패스워드와 패스워드 해시가 일시적으로 호스트의 메모리나 임시(스왑) 파일 등에 저장된다. 패스워드와 해시가 저장될 때 이들 자원에 접근한 공격자는 패스워드를 잠재적으로 패스워드 추출 유틸리티 등을 이용하여 복구 할 수 있다.

고 위험 호스트를 가진 각 조직은 이들 패스워드와 해시가 일시적으로 얼마동안 저장되는지와 적절하게 제거되는지를 평가 할 필요가 있다.

패스워드를 호스트에 저장하는 외에 사용자와 관리자는 종이에 패스워드를 기록해 둘 수도 있으며, 이는 패스워드를 기억할 필요가 없게 한다. 이와 같이 종이에 기록하는 것은 물리적으로 안전해야한다. 즉 금고 등과 같은 안전한 장소에 저장함으로서 물리적인 탈취로부터 보호 할 수 있어야 한다. 또한 패스워드가 만료되었을 때 기록된 종이는 파쇄기 등을 이용하여야 한다.

2) 전송

패스워드와 패스워드 해시들은 호스트사이에 인증 시 내외부 네트워크를 통하여 전송된다. 패스워드와 해시가 전송 될 때 가장 큰 위협은 유무선 네트워크 통신 시 도청하는 스니핑(sniffing)이다.

스니핑은 수동적 도청이나 능동적 가로채기, 즉 두 개의 사른 시스템 사이에 메시지가 통과 될 때 중간에서 가로채는 것이다. 대부분의 스니퍼들은 패킷 구조를 알고 있다면 수집된 데이터를 분석하고 해독 할 수 있다. 스니퍼들은 텔넷, FTP, POP3(Post Office Protocol 3), HTTP 등과 같은 프로토콜에 의해서 비 암호화되어 전송되는 사용자 이름과 패스워드를 수집 할 수 있다.

또한 패스워드 보호를 위해 사용된 결함이 있는 암호 알고리즘 구현은 공격자가 쉽게 우회 할 수 있다. 어떤 스니퍼들은 수진된 정보로부터 자동적으로 사용자 이름과 패스워드를 추출하여 계정정보와 데이터를 알아보기 쉽게 정돈된 형태로 관리한다. 그러한 스니퍼들은 패스워드 해시를 식별하여 크랙을 시도 할 수 있다.

스니핑 위협은 다음과 같은 방법을 포함하여 여러 가지 방법으로 완화 시킬 수 있다.

① TLS(Transport Layer Security) 같은 것을 사용하여 패스워드나 패스워드를 포함하는 통신을 암호화 하거나, VPN(virtual private network)을 통한 터널링 하기.

② 평문 패스워드 대신에 암호화 패스워드 해시 전송하기.

③ 패스워드를 보호하지 않는 프로토콜을 패스워드를 보호하는 프로토콜로 전환하기.

예를들면 텔넷을 SSH(Secure Shell)로, HTTP를 HTTPS (HTTP Secure)로 전환하는 것이다.

④ 내부 네트워크상에서 전송되는 패스워드를 보호하기위해서 네트워

크 분리와 완전한 스위치 네트워크 사용하기. 이 방법은 스니핑의 가능성을 제거하지는 않고 감소시킬 뿐이다.
⑤ 스니핑에 노출되는 패스워드 구현방법을 Kerberos 같은 보다 안전한 패스워드 기반인증 프로토콜로 대체하기.

스니핑의 위협 때문에 패스워드와 패스워드해시가 중요한 자원에 접근하는데 사용되는 경우에 부가적인 암호화 과정 없이 신뢰되지 않는 네트워크에서 전송되어서는 안 된다.

패스워드 전송 시 또 다른 위협은 재연 공격(replay attacks)으로 공격자가 원래 트래픽의 응답인 것처럼 가로챈 트래픽에 재송신하는 방법이다. 패스워드가 포함되어 있을 때 재연공격은 정당한 증명 없이 정보에 접근하기를 시도 할 수 있다. 예를 들면 공격자가 어떤 암호화된 인증서를 포함하고 있는 패킷을 스니핑 할 수 있다면 공격자는 암호화된 인증서를 재송신 할 수 있고(복호화 필요 없이), 인증 프로토콜이 재연공격에 취약하다면 이 인증서에 의해 인증 될 수 있다. 많은 조직들은 인증 패킷에 타임스탬프 등을 결합한 인증 프로토콜을 사용하거나, TLS 같은 보호프로토콜에 인증 프로토콜을 포장하여 재연방지를 하여 비 신뢰 네트워크에 대한 공격을 완화 시킬 수 있다.

3) 사용자 지식정보와 행위

패스워드들은 사용자 지식정보와 행위를 이용하여 탈취 될 수 있다. 사용자가 패스워드를 컴퓨터에 입력 할 때 패스워드가 어깨 넘보기(shoulder surfing) 같은 비-기술적인 방법으로 탈 취 될 수 있다.
사용자는 패스워드를 입력하기전이나 입력 하는 중에 이와 같은 어깨 넘보기를 인식하고 있어야한다.
패스워드 입력은 기술적인 수단으로 공격자가 모니터할 수 있다. 즉

"키 로거"라고 하는 키 입력 저장기(keystroke logger)는 키보드 자판에서 입력하는 모든 자판을 모니터하는 기능이다. 공격자는 키 로거를 통하여 사용자이름과 패스워드를 알 수 있다. 많은 트로이 목마와 같은 악성 프로그램은 사용자이름, 패스워드, 기타 중요한 정보들을 모니터한다.

이와 같은 종류의 위협은 사용자의 호스트를 효율적으로 안전하게 함으로서 완화 시킬 수 있다. 즉 정기적인 패치, 바이러스 백신 설치, 관리자 레벨에서 작업하지 않고 사용자 레벨에서 작업하기 등이다. 또 다른 완화 기법은 패스워드 타이핑을 피하는 방법이다. 즉 안전한 저장장치로부터 패스워드를 검색한다거나, 스크린상에 가상 키보드를 띄워 패스워드를 입력하는 방법이다. 또한 사용자는 악성 소프트웨어를 통한 공격을 인식해야한다. 알지 못하는 곳으로부터의 다운로드 안하기 같은 악성 소프트웨어를 회피하는 방법을 인식해야한다. 또한 공개적으로 누구나 사용할 수 있는 컴퓨터(호텔, 컨퍼런스 등의 컴퓨터)에서 사용자는 패스워드 사용을 자제해야한다. 가장 고 위험군에 속하기 때문이다.

또한 사용자는 사회 공학적(Social Engineering) 방법으로 패스워드가 누설 될 수 있다. 예를 들면 공격자는 도움이를 가장하거나 문제점을 해결하는데 필요한 패스워드를 요구 할 수 있다. 사회 공학적 공격은 많은 형태가 있다. 악성 웹 사이트를 합법적 사이트로 위장하여 사용자의 피싱 전자우편 등과 같은 기술적 방법도 여기에 속한다. 많은 피싱 공격의 목적은 사용자로부터 사용자이름과 패스워드, 기타 민감정보를 수집하는 것이다. 사회 공학적 공격 위협을 완화시키는 것은 기술적인 통제방법(많은 웹 브라우저는 피싱 백신을 갖추고 있다)이 있다고 하여도 그와 같은 위협을 인식하고 사용자가 어떻게 정보를 취급해야하는지를 알고 있어야한다.

사회 공학적 공격은 지원창구나, 시스템 관리자, 기타 계정 권한을 가진 IT 관리자로 위장하기 때문에 각 조직은 그런 공격을 어떻게 인

지하고 어떻게 대응할 것인지를 준비해야한다.

사용자와 관련하여 패스워드가 노출되는 또 다른 문제는 악의적인 내부자(전 현직 조직 불만 고용자)다. 그들은 정당한 페스워드를 알고 있고 다른 부서와 패스워드를 공유 할 수 있다. 악의적인 내부자는 인증 과정과 보호방법, 부분적 취약점 등을 암시적으로 누설하게 한다. 사용자는 특별히 권한이 부여되지 않은 동료에게 시스템에 접근을 허용하는 우를 범 할 수 있다.

2. 패스워드 추측과 크래킹

공격자들은 추측과 크래킹이라는 두 가지의 기술적 방법을 통하여 패스워드 해시로부터 패스워드를 복구하고 취약한 패스워드 찾기를 시도 한다.

추측은 기본설정 패스워드. 사전단어, 기타 가능한 조합 등을 사용하여 반복적으로 인증을 시도하는 개념이다. 크래킹은 공격자가 해시를 생성할 문자 스트링을 식별하기 위해서 다양한 분석방법을 이용하여 암호화된 패스워드 해시를 복원하기위한 과정이라고 말 할 수 있다. 추측은 인증 인터페이스를 접근 할 수 있는 공격자에 의해 시도될 수 있으며, 크래킹은 패스워드 해시에 이미 접근한 공격자에 의해서 시도 될 수 있다. 여기에서는 추측과 크래킹에 대한 위협을 완화 할 수 있는 전략을 언급한다.

1) 추측

추측에는 여러 형태가 있다. 무차별 공격(brute force attack)형태는 공격자가 주어진 패스워드 길이까지를 주어진 문자를 이용하여 가능한 모든 조합을 사용하여 패스워드 추측을 시도하는 개념이다. 이 방법은

많은 조합이 시도되어야 하기 때문에 많은 시간이 소요된다. 사전공격(dictionary attack)형태는 공격자가 기능한 패스워드 리스트를 사용하여 패스워드 추측을 시도하는 방법이다. 이 리스트는 숫자, 문자, 심볼들을 포함하지만 패스워드를 생성하기 위해서 가능한 모든 조합을 사용하지는 않는다. 복합공격(hybrid attack)형태는 공격자가 패스워드 가능성 있는 사전(숫자, 문자, 심볼)을 사용하여 이를 무차별 공격방법으로 패스워드 추측을 시도하는 방법이다. 여기에서 공격자는 일정한 방법으로 규칙적으로 문자를 추가하거나 대체하는 방법을 사용하기 때문에 일반적인 무차별 공격방법보다는 시간소비가 적지만 사전공격방법보다는 좀 더 많은 시간을 필요로 한다. 추측공격의 또 다른 형태는 목적하는 대상자의 가족수, 생년월일, 자동차번호, 주민번호 등 주변정보를 탐색하여 패스워드를 찾는 방법이다. 추측공격은 두가지방법을 조합함으로서 보다 쉽게 완화 시킬 수 있다.

첫째는 패스워드를 아주 복잡하게 구성하여 공격자가 읽을 수 없게 하는 방법이다. 특히 OS나 어플리케이션 프로그램의 기본 패스워드를 변경시키는 경우에 이 개념은 아주 중요하다. 공격자가 자주 사용하는 것이 기본 계정과 패스워드 목록이기 때문이다. 각 조직은 계정이름이나 사용자이름 같은 평범한 집합이나 단순한 키보드 조합패턴(예 : "1234!@#$", "qwerty") 이나 날짜(예 : "03012010"), 사전단어, 사람이나 장소 등을 사용 할 수 없게 해야 한다. 대부분의 패스워드 메커니즘은 이와 같은 패스워드 사용을 방지하고 있다.

둘째는 OS와 어플리케이션 패스워드 인증 메커니즘에서 인증 시도를 제한하도록 구성하여 공격자의 추측공격을 완화하는 방법이며, 그 예는 다음과 같다.

여러 번의 인증시도(특정시간 내) 실패는 그 이용계정을 잠기도록 한다. 예를 들면 사용자가 연속적으로 패스워드를 50회 시도하여 실패 했다면 그 후에 그 계정에 대한 모든 인증시도는 15분 동안 무시하는 방

법이다. 단지 몇 번의 인증시도 실패 후 잠김은 정상적 사용자에게 보다 단순한 패스워드를 사용하는 원인을 제공하거나 안전하지 않은 방법인 다른 곳에 기록하는 원인을 제공하는 등 의 문제를 야기 시킨다.

인증 시도 실패시마다 다시 시도하기까지 기하급수적으로 일정시간 동안 지연시킬 필요가 있다. 예를 들면 첫 번째 인증시도 실패는 5초의 지연시간 후에 다음시도를 하게하고, 두 번째 인증시도 실패는 10초의 지연시간 후에 다음시도를 하게하고, 세 번째 인증시도 실패는 20초의 지연시간 후에 다음시도를 갖게 하는 방법이다.

추측은 공격자에게 패스워드에 대한 정보를 부주의로 제공하는 패스워드 메커니즘에 의해 쉽게 가능하다. 예를 들면 그 정보는 패스워드가 입력될 필드에 최대 8자의 문자를 입력하도록 미리 정해져 있을 경우에 패스워드의 길이 정보기능이나, 이용자계정에 대한 존재여부를 알려주는 기능이나, 최소 몇 자 이상의 패스워드가 입력 될 때 승인한다든가 등을 말한다. 이 정보는 신규 패스워드를 생성 할 때 인증된 사용자에게 매우 유용한 정보이지만, 합법적 사용자에게 주는 이익보다는 공격자에게 더 많은 이익을 주게 된다.

패스워드 추측의 특별한 경우는 패스워드 재설정을 위해서 계정을 최초로 생성 할 때의 기본설정 패스워드를 사용하는 것이다. 패스워드 재설정은 일회용 패스워드(one-time password : OTP)를 설정하여 이용한다. OTP를 어떻게 사용하는지의 예로는 신규계정 생성 담당자가 OTP를 생성하여 사용자에게 제공하는 것이다. 그 때 사용자는 단 한 번만 그 패스워드로 로그인 하게 되고 파기되며 신규 패스워드 설정을 필요로 한다. 난수로 생성되거나 선택된 OTP가 계정 생성이나 패스워드 재설정 과정에 사용 되어야한다. 이것은 사용자가 할당된 OTP를 변경시키지 않으면 그 패스워드는 쉽게 추측 할 수 없다. 어떤 자동화된 절차에서는 난수 OTP가 생략 될 수 있다. 왜냐하면 사용자가 시스템에 자신의 신분을 검증한 후에 즉시 신규 패스워드를 설정하기 때문

이다. 지원창구나 보안 담당자가 신규 패스워드를 설정하는데 동행한다면 난수 OTP는 불필요 할 수도 있다.

2) 크래킹

크래킹은 목표로 하는 패스워드와 같은 암호화된 해시를 생성 할 문자 스트링을 찾는 행위를 포함한다. 발견된 스트링은 실제 패스워드이거나 동등의 해시를 생성하는 다른 패스워드일수 있다.

만약 해시 알고리즘이 취약하다면 크레킹은 보다 쉽게 된다. 해시함수는 단방향 이어야한다. 그렇지 않으면 해시에 접근할 수 있는 공격자는 해시 함수로부터 패스워드를 식별 할 수도 있다. 해시 알고리즘 취약성의 또 다른 예로서 어떤 알고리즘은 설팅(salting)을 사용하지 않는 것이다. 설팅이란 해시함수와 동등한 패스워드의 가능성을 최소화시키기 위해서 패스워드 해시 과정에 난수값을 포함시키는 것이다. 만약 두 명의 이용자가 같은 패스워드를 선택했다면 설팅은 그 해시들을 최대한 상이하게 만들 수 있다

크레킹 기술을 사용하는 공격자들은 가끔 무지개 테이블(rainbow tables)이라는 것을 사용한다. 이것은 사전에 계산된 패스워드 해시를 포함하는 검사테이블을 의미한다. 이 테이블은 공격자가 목표시스템에 최소의 시간으로 패스워드 크랙 시도를 가능하게 하여 복수의 계정을 크랙 할 때 해시를 재성성하지 않고 공격할 수 있게 한다. 예를 들어 공격자는 주어진 문자집합이 어떤 길이의 문자를 구성하는 모든 치환정보를 포함하는 무지개 테이블을 생성하거나 취득한다. 그때 공격자는 두 개로 구분된 패스워드 해시 파일 대신에 이 테이블을 사용한다. 즉 이전에 생성되어 있기 때문에 치환을 이중으로 생성하지 않게 된다. 이것은 공격자가 해시를 계속 생성하는 대신에 검사 테이블을 이용함으로서 보다 신속하게 크래킹을 수행할 수 있도록 하고 다시 계산하는 문제를 해결해준다.

무지개 테이블의 사용과 관련해서는 몇 가지 이슈가 존재한다. 이것은 대용량의 저장장치와 아주 긴 생성시간이 필요하다는 것이다. 후자는 공격자가 이전에 생성된 테이블을 재사용하거나 존재하는 테이블을 복사하여 사용 할 수 있다면 그다지 중요한 문제는 안 된다. 또한 무지개 테이블의 사용은 설팅을 사용함으로서 방지 할 수 있다. 공격자가 계정에 설팅을 포함하지 않으면 무지개 테이블들은 정확한 값을 생성하지 않게 되며, 테이블이 요구하는 공간은 기하급수적으로 증가하게 되어 대규모의 절임(설팅)은 무지개 테이블의 사용을 불가능하게 만들 수 있다. Mac OS X 와 다른 Unix-based OS 같은 운영체제에서는 패스워드 크레킹을 효과적으로 억제하기위해서 절임 패스워드 해싱 메커니즘으로 구현되어 있다. 무지개 테이블의 사용을 완화시키는데 도움을 주는 또 다른 기술은 스트레칭(stretching) 이다. 스트레칭은 각 패스워드와 절임을 수천 번 해싱하는 것이다. 이것은 무지개테이블의 생성시간을 최대한 길게 하는 것이다.

모든 형태의 크래킹은 패스워드를 강력하게 구성하고,. 단방향 패스워드 해시 알고리즘을 사용하고, 패스워드 해시의 비밀을 유지함으로서 완화 시킬 수 있다. 정기적인 패스워드변경은 크래킹의 위험을 완화시키는데 도움이 된다. 3.2.3에서 이들의 완화 기술을 언급한다.

3) 패스워드 강도

강한 패스워드는 추측과 크래킹을 완화시킨다. 패스워드 강도는 패스워드의 길이와 문자의 예측 불가능한 복잡성에 의해 결정된다. 패스워드 복잡성 정책의 예는 패스워드를 구성할 때 소문자, 대문자, 숫자, 특수문자의 4 가지 중 적어도 3가지의 조합으로 구성하도록 하는 것이다.

표 3-1은 패스워드와 복잡성의 효과를 설명한다. 다양한 길이와 문자 집합을 사용하여 패스워드를 구성한 경우이다. 키보드 자판은 가능한 킷값의 집합이다. 예를 들어 4자리 PIN은 10개(0부터9까지)의 각기 다

른 값의 일부이다. 여기에서 가능한 키 값은 10,000개(0000-9999)이다. 95개의 문자 집합을 사용하여 8자리 패스워드는 95^8개의 가능한 값(약 $7*10^{15}$)을 가진다. 무차별 공격에서는 자판이 증가 할수록 그만큼 많은 시간을 소비하게 된다.

표는 자판이 증가함에 따라 복잡도가 급속하게 증가됨을 보여준다. 4개 문자열을 갖는 패스워드를 기준 할 때 26개 문자집합에서 95개 문자집합까지 문자집합의 증가는 거의 200배의 키 값 수가 증가한다. 그러나 패스워드의 길이가 4에서 12로 증가한다면 단지 26개의 문자집합을 기준으로해도 키 값은 거의 2조배로 증가한다. 무차별공격과 암호공격을 억제하기위해서 패스워드 강도에 의미 있는 영향을 가지는 것은 패스워드의 길이이다. 패스워드길이가 8자에서 15까지 허용되어 사용되고 있다. 패스워드의 길이를 작게 하는 것은 키 공간과 밀접한 관련을 가진다. 예를 들어 6자에서 8자까지 범위는 사용자의 패스워드 선택을 제한하게 한다.

<표 3-1>에 나타낸 키 공간은 이상적인 가능한 패스워드이다. 즉 가능한 모든 집합을 가정한 것으로 실제 사용되지 않는 경우를 포함 하고 있다. 자신이 패스워드를 구성하는 사용자는 어떤 패턴을 따르고 있다. 즉 시스템이 대/소문자와 숫자를 포함하여 최소 8자 길이의 패스워드를 요구 한다면 사용자는 최소의 길이로 첫 글자는 대문자로 나머지는 소문자로, 끝에는 숫자로 구성하는 패턴형식을 가지는 예를 들 수 있다(예: Univ2010). 또 다른 패턴으로는 특정문자를 숫자로 대체(예: 문자 l을 숫자 1로, 문자 O를 숫자 0으로 대체) 하여 사용하고, 패스워드의 마지막에 특수문자를 덧붙이는 방식을 사용 할 수도 있다. 이와 같은 패턴을 기반으로 하는 패스워드는 패스워드의 복잡성과 요구하는 길이를 충족시키지만, 공격자는 이런 패턴을 인식하고 있기 때문에 의미 있는 키 값 수를 감소시키게 된다. 유사한 문제점으로는 사용자가 간단한 상용구(잘 알려진 제목 등)를 많이 사용함으로서 길이는 충족하

지만 연속적인 사전식 단어로 구성되어 균질성이 떨어진다.

<표 3-1> 문자집합과 패스워드 길이를 고려한 키 값 공간

문자 집합 크기	문자형태				패스워드 길이				
	숫자	문자	특수문자	기타	4	8	12	16	20
10	10진수				$1*10^4$	$1*10^8$	$1*10^{12}$	$1*10^{16}$	$1*10^{20}$
16	16진수				$7*10^4$	$4*10^9$	$3*10^{14}$	$2*10^{19}$	$1*10^{24}$
26		대/소 문자 구분 없음			$5*10^5$	$2*10^{11}$	$1*10^{17}$	$4*10^{22}$	$2*10^{28}$
36	10진수				$2*10^6$	$3*10^{12}$	$5*10^{18}$	$8*10^{24}$	$1*10^{31}$
46	10진수		10 개 (숫자 버튼위)		$4*10^6$	$2*10^{13}$	$9*10^{19}$	$4*10^{26}$	$2*10^{33}$
52		대/소 문자 구분			$7*10^6$	$5*10^{13}$	$4*10^{20}$	$3*10^{27}$	$2*10^{34}$
62	10진수				$1*10^7$	$2*10^{14}$	$3*10^{21}$	$5*10^{28}$	$7*10^{35}$
72	10진수		10 개 (숫자 버튼위)		$3*10^7$	$7*10^{14}$	$2*10^{22}$	$5*10^{29}$	$1*10^{37}$
95	10진수		표준 키보드의 모든 특수문자		$8*10^7$	$7*10^{15}$	$5*10^{23}$	$4*10^{31}$	$4*10^{39}$
222	10진수			기타 모든 ASCII 문자	$2*10^9$	$6*10^{18}$	$1*10^{28}$	$3*10^{37}$	$8*10^{46}$

정보시스템에서 균질성이란 시스템에서 무질서성(난수성)을 측정하는 개념이다. 균질성이 부족한 패스워드는 무차별 공격에 보다 취약한 특성을 가진다.

패스워드 길이와 복잡성을 위한 정책을 결정할 때 각 조직은 최대의 실제 킷값 수를 고려해야한다. 사용자가 자신의 패스워드를 기억하기 기대한다면 보다 기억하기 쉽게 패스워드정책에서 고려해야한다. 만약 패스워드가 다른 곳에 저장되어 기억하지 않아도 되는 경우라면 길이와 복잡도를 극대화해야 한다. 패스워드길이와 복잡도 정책에서 고려해

야 할 또 다른 중요사항은 크레킹 공격이 수행되는 비율이다.

또한 각 조직은 패스워드 강도 요구사항을 어떻게 효과적으로 강제화 할 것인지를 고려 할 필요가 있다. 많은 운영체제와 어플리케이션들은 모든 요구사항을 준수 할 수 없을지도 모른다.

이와 같은 상황에서 준수율을 향상시키기 위한 방법은 패스워드 필터 기능을 추가하는 것이다. 즉 패스워드가 패스워드 정책에 따르는지를 검증하도록 설계된 기능을 추가하는 개념이다. 여기에서 패스워드가 취약하다면 다른 패스워드를 선택하도록 할 수 있다. 비교적 정밀성이 낮은 솔루션은 사용자에게 패스워드강도 요구사항과 패스워드 강도 요구사항을 위반한 취약한 패스워드는 크렉커에 의해 정기적으로 검사되고 있음을 교육해야한다.

이런 솔루션은 패스워드 필터 같은 사전검증 솔루션의 실행이 어려울 때만 사용되어야하며, 이때 각 조직은 패스워드 강도 요구사항 변경이 필요할 때 보다 쉽게 적용할 수 있어야 한다.

예를 들어 시스템이 패스워드에 구두점 사용을 금지하고 있다면, 길이가 좀 더 긴 패스워드 사용을 요구 할 수 있다. 이것은 패스워드 길이요구사항을 증가시킴으로서 보다 안전성을 향상시키지만 구두점 사용을 하지 않음으로서 복잡도는 저하되게 된다.

정책을 수립 할 때 각 조직은 패스워드 길이와 복잡도 요구사항을 손상시킬 수 있는 패스워드 메커니즘으로 인하여 계정 취약이 발생 할 수 있다. 그 예는 다음과 같다.

어떤 패스워드 메커니즘은 사용자가 기대보다 제한된 문자집합을 가진다. 즉 어떤 어플리케이션은 사용자가 대/소문자를 이용한 패스워드를 패스워드 해시가 수행되기 전에 대문자나 소문자로 통일하여 모두 변환시키기도 한다. 이것은 사용자가 생각했던 것보다 패스워드의 강도를 저하시키는 결과를 초래한다.

또 어떤 패스워드 메커니즘은 저장되거나 검사되는 최대 길이보다

더 긴 패스워드 입력을 허용한다. 입력 길이를 알지 못하는 사용자는 자신도 모르는 사이에 취약한 패스워드를 만드는 결과를 초래한다. 사용자로부터 임의의 긴 패스워드를 받아드린 시스템이 해시를 수행하기 전에 8자로 절사시키는 경우가 그 예이다. 즉 사용자가 "Security is my #1 Priority!"라는 패스워드로 설정 했다면 그 시스템은 사용자가 생각했던 패스워드보다 훨씬 취약한 "Security"라는 패스워드로 인식하는 결과를 초래한다.

4) 사용자 패스워드 선택 방법

패스워드 생성에는 자동 난수 생성(pseudo-random)방법과 사용자 생성방법이 있다.

자동 난수 생성 방법이 사용자 생성 패스워드보다 고도의 균질성을 제공하고 보다 강도가 높지만, 사용자는 기억하기 더 힘들 수 있다. 반대로 사용자 생성 패스워드는 균질성이 떨어지고 좀 더 추측과 크레킹에 취약하지만, 사용자가 기억하기 용이하다. 사용자가 패스워드를 기억 할 필요가 없는 경우에는 자동적으로 생성된 패스워드를 사용하는 것이 가능하다. 패스워드 생성 유틸리티가 이때 패스워드를 생성 할 때 사용 될 수 있다. 보통 패스워드 생성기는 패스워드 제한이 되어있으며, 사용자의 제한요구를 허용하고 있다. 즉 패스워드 생성기는 그 제한 조건을 수용하여 패스워드를 생성하게 된다. 자동적으로 생성된 패스워드는 모든 가능한 문자집합(대문자, 소문자, 숫자, 특수문자)을 이용하여 가능한 한 최대 길이로 강력하게 구성된다. 이것은 사용자가 현실적으로 기억하기가 어렵다. 기억하기 용이한 패스워드가 되려면 각 조직은 보안 필요성과 기대하는 사용자 태도를 고려하여 패스워드 생성방법을 결정해야한다.

사용자가 신규 패스워드를 선택 할 필요가 있을 때, 사용자 선택이나 난수 생성이든지 상관없이 패스워드 구성에 관한 제한을 포함해서 패

스워드 요구사항을 인식해야한다. 예를 들면 어플리케이션이 문자와 숫자의 조합으로 8자에서 20자까지 사이의 패스워드 길이를 허용하며, 마침표 같은 특수문자는 금지 할 수 있다. 패스워드 제한에 대한 명확한 목록을 제공하는 것은 사용자에게 패스워드 기준을 충족하는 패스워드 선택을 지원하며, 신규 패스워드가 거부되는 불편을 해소해준다.

각 조직은 구성원들에게 강력한 패스워드의 특성과 중요성을 인식하도록 교육 등을 실시해야한다.

강력하고 상대적으로 기억하기 쉬운 패스워드를 사용자가 선택 할 수 있도록 여러 방법들이 개발 되어 있으며, 그 방법들을 나열하면 다음과 같다.

① 연상방법 :

사용자는 관용구를 선택하고 관용구의 각 단어중 하나의 문자(즉 각 단어의 첫 번째나 두 번째 문자)를 추출하는 방법에 숫자나 특수문자 등을 추가하는 방법이다. <표 3-2>는 이와 같은 연상방법의 예를 나타낸 것이다.

<표 3-2> 패스워드 생성의 연상방법

관 용 구	패스워드
우리나라 좋은 나라.	Dfsfwdsf.(한글자판, 첫 자는 대문자)
This is the worst car I have ever driven in my LIFE!	TitwcIhedimLIFE!
I am definitely your #1 fan.	Iady#1f.

연상방법이 사전식 패스워드보다는 일반적으로 좀 더 강력하지만, 무차별 추측공격에는 노출될 수 있다. 보통사용하지 않는 문자로 대치하

지 않고 평범한 관용구를 연상 패스워드로 변환한다면 연상패스워드 사전을 사용하는 공격자에게는 추측 될 수 있다. 사용자는 생성 연상 패스워드에 평범한 관용구를 피하고 자신의 관용구를 만들어 대문자, 마침표, 단어에서 한자, 혹은 두자를 뺀다든지 하는 예측 불가능한 변환을 해야 한다.

② 관용구 변경방법 :

사용자는 관용구를 선택하고 그 관용구의 파생의 형태로 치환하는 방법이다. 이 방법은 길고 복잡한 패스워드 구성을 하게 한다. 관용구는 패스워드의 구조에 비교 할때 기억하기 쉽다. <표 3-3>은 관용구 변경방법의 예를 나타낸 것이다.

<표 3-3> 관용구 변경방법 예

관 용 구	치환변경된 관용구
to be or not to be	2.be.0r.nOt@to0.bEE
Dressed to the nines	Dressed*2*the*9z

연상 패스워드와 마찬가지로 생성된 변경 관용구로 평범한 관용구 사용을 피하고 예측 불가한 변경이 필요하다.

③ 단어의 결합과 변경 방법 :

사용자는 두 세개의 서로 관련 없는 단어를 결합하고 이들 문자의 일부를 숫자나 특수문자로 변경하는 것이다. <표 3-4>는 결합된 예를 보여준다.

<표 3-4> 결합과 단어 변경

단어	패스워드
“bank” and “camera”	B@nkC@mera
“mail” and “phone”	m4!lf0N3

또 다른 전략은 하나의 기억 할 수 있는 기본 패스워드를 선택한 후 여기에 문자나 특수기호를 추가하는 것과 같은 파생어의 형태로 변경하는 방법이다. 각 파생어는 다른 시스템이아 어플리케이션의 패스워드 사용 할 수 있다. <표 3-5>는 파생어의 예를 보여준다.

<표 3-5> 파생어를 이용한 패스워드

파 생 어	시스템 혹은 어플리케이션	패스워드 결과
기본 패스워드	없음 (기본 패스워드는 다른 패스워드를 만들때 만 사용하며, 실제 사용하지는 않는다)	G00dTimes
기본 앞에 “42*” 추가	시스템 1	42*G00dTimes
기본 뒤에 “*42” 추가	시스템 2	G00dTimes*42
기본앞에 “42*” 추가하고 중간에 “#23” 삽입	어플리케이션 1	42*G00d#23Times

사용자는 기본 패스워드만을 기억하고 모든 파생어 규칙을 기억 할 필요가 없으며, 필요한 패스워드를 유추 할 수 있는 규칙과 파생 규칙을 기록 해 둘 수 있다. 그러나 이 방법에는 두 가지의 단점이 있다. 만약 공격자가 그 규칙에 접근했다면 공격자는 쉽게 패스워드를 추측하거나 크레킹 할 수 있다. 또한 공격자가 패스워드 중 하나만 알고 있

으면 다른 패스워드도 쉽게 알 수 있다는 것이다. 따라서 사용자의 어깨 너머로 패스워드 입력을 엿보거나 규칙 기록을 열람한 공격자는 작은 노력으로 여러 계정에 접근 할 수도 있다.

5) 로컬 관리자 패스워드 선택 방법

대부분의 기업에는 두 가지 형태의 패스워드가 있다. 즉 로컬과 도메인이다. 도메인 패스워드는 인증서버(예 : 단순 디렉토리 접근 프로토콜 서버, 액티브 디렉토리 서버)에서 인증되는 중앙 집중화된 패스워드이다. 로컬 패스워드는 로컬 시스템(워크 스테이션이나 서버)에 저장되어 인증되는 패스워드이다. 대부분의 로컬 패스워드가 중앙 집중화된 패스워드 관리 메커니즘을 사용하여 운영된다고 해도, 일부는 제 3의 도구, 스크립트, 수작업으로 운영 될 수 있다. 통상적인 예로는 내장된 관리자와 루트 계정이다.

하나의 네트워크 내 모든 기계의 로컬 관리자와 루트 계정 중에 공용하는 통상적인 패스워드를 가지는 것은 시스템의 관리를 단순화 시켜주지만, 광범위한 취약이 있다. 만일 하나의 기계가 위태롭게 되면 공격자는 그 기계를 공격하여 패스워드를 복구하고, 공유된 패스워드를 사용하는 다른 기계에 접근하여 사용 할 수도 있다. 각 조직은 동일한 로컬 관리자나 루트 계정 패스워드를 여러 시스템에 같이 사용해서는 안 된다. 또한 내장된 계정은 패스워드 정책이나 필터에 악영향을 주지 않기 때문에 내장된 계정을 폐쇄하고 대신에 관리자 수준의 계정을 사용 할 수도 있다. 이런 로컬 패스워드관리 문제에 관한 제품은 가끔 각 기계에 유일한 생성된 패스워드를 사용하고, 클라이언트 기계에서 로컬 패스워드를 유지하는데 사용되는 중앙 집중된 패스워드 데이터베이스를 사용한다. 이와 같은 데이터베이스는 강한 안전성이 있어야하며, 최소의 필요성을 기반으로 접근 되어야만 한다.

특히 보안은 인증된 호스트로부터 데이터에 접근하기위해 인증된 관

리자만을 허용하도록 통제한다. 로컬 계정 패스워드 관리의 또 다른 제품은 기계이름이나 MAC(media access control)주소 같은 시스템 특성을 기반으로 패스워드를 생성하는 것이다. 예를 들면 로컬 패스워드는 MAC주소와 표준 패스워드의 암호화 해시로 구성 될 수 있다.

어떤 기계의 MAC 주소가 "00:16:59:7F:2C:4D"이고 표준 패스워드가 "AanTiRul309"라면 스트링 "00:16:59:7F:2C:4D AanTiRul309"으로 결합될 수 있다.

이 스트링은 그 기계의 패스워드로서 사용되는 처음 20자를 SHA를 사용하여 해시 될 수 있다. 이것은 공유된 패스워드를 공격자가 알아내는 것을 예방하는 수단이 된다. 그러나 공격자가 로컬 패스워드를 복구했다면 상대적으로 쉽게 패스워드가 노출 될 수 있다.

어떤 방법을 선택하는 문제와는 별개로 여러 시스템에 공유하여 로컬 계정 패스워드 사용을 예방하도록 구현 하여야만 한다.

3. 패스워드 변경

공격자는 자기가 설정한 패스워드로 기존의 패스워드를 변경하여 계정에 성공적으로 인증 될 수 있다. 공격자는 기존의 패스워드를 알 필요가 없게 된다. 여기에서는 공격자가 계정에 접근하는 패스워드를 변경하는 여러 가지 방법을 고찰한다.

1) 패스워드 분실 복구와 초기화

사용자가 패스워드를 잊었을 때 일반적으로 두 가지 선택이 있다. 즉 과거 패스워드를 되찾기(패스워드 복구)와 신규 패스워드로 초기화(패스워드 리셋)이다.

패스워드 초기화는 최초의 패스워드를 설정하기 위하여 생성 될 때

수행된다. 패스워드 복구와 리셋 수행에는 여러 가지 방법이 있다. 즉 IT 관리자를 사람이 직접 방문하는 방법부터 자동 서비스방법까지 다양하다. 사용자가 요구하는 패스워드 복구와 리셋이 적정하게 검증 되지 않으면 공격자는 사용자의 패스워드를 쉽게 얻게 되는 것이다. 따라서 모든 복구와 리셋 메커니즘은 사용자를 식별하는 검증이 우선 수행되어야 한다. 여기에는 기본 지식 기반 검증(예 : 주민번호, 신분증번호 등), 계정 설정 당시 작성된 질의 답변(고향, 첫 번째 차량 색, 좋아하는 애완동물 등), 등록된 핸드폰으로 인증번호 전송하기, 면담을 통한 사진으로 확인하기 등 여러 가지 방법이 있다.

각각의 검증 방법들은 장단점이 있다. 프라이버시와 관련사항은 주의 깊게 취급되어야 한다. 예를 들면 주민번호와 신용카드번호 같은 정보가 신분 검증에 사용되어서는 안 된다. 사용자 검증은 공격자가 추측하거나 쉽게 얻을 수 있는 데이터나 질의응답(예: 회사의 고용번호)을 포함해서도 안 된다. 각각의 패스워드 복구와 리셋 메커니즘에서 사용자 검증의 충분성은 계정의 보안 필요성과 상대적으로 검토되어야 한다. 예를 들면 각 조직이 고도의 보안 패스워드가 필요하다면 엄격한 검증 방법이 필요하며, 그렇지 않으면 덜 엄격해도 된다. 검증 방법을 선택 할 때 각 조직은 각 방법의 비용과 편의성을 고려한 상대적인 위험을 고려해야한다. 또한 각 조직은 물리적으로 멀리 있는 사람에 대한 복구와 리셋을 수 행 할 때 요구사항을 설정하고 식별해야한다.

패스워드 복구와 리셋 중에 저장되고 전송되는 모든 민감 정보의 기밀성은 보호되어야한다. 예를 들면 사전 등록된 질의응답이나 패스워드 힌트 질문이 신분 확인에 사용 된다면 그 답변에 대한 기밀성은 항상 보호되어야 하며, 그 질문이 사용자 생성 질문인지, 기타 다른 방법의 생성 질문인지도 보호되어야 한다. 각 조직들은 질의응답 내용이 암호화되는지를 확인 할 필터 사용을 주의 깊게 고려해야한다. 평문의 전자우편으로 패스워드가 전송되어서는 안 된다.

2) 저장된 계정 정보와 패스워드에 대한 접근

공격자는 저장된 사용자 계정정보와 패스워드에 접근하여 패스워드를 변경 할 수 도 있다. 예를 들면 어떤 호스트가 패스워드 파일에 대한 부정확한 권한 설정을 한 경우 사용자는 패스워드를 덮어쓰기 할 수도 있어, 다른 계정이나 신규 계정을 생성하여 신규 패스워드를 설정할 수 있다. 공격자가 호스트에 물리적 접근이 가능하다면 많은 호스트에서 유사한 공격이 발생 할 수 있다. 물리적으로 접근한 공격자가 내장된 관리자 계정 패스워드를 리셋 시킬 수 있는 패스워드 리셋 도구와 유틸리티가 있기 때문이다.

봇넷을 통하여 많은 컴퓨터의 가용성을 침해하고 소프트웨어 크레킹하기 때문에 공격자들은 항상 패스워드를 크렉할 수 있는 능력을 키우고 있다. 패스워드 해시에 사용된 암호 알고리즘의 형태가 어느 정도 크레킹 속도에 영향을 미치지만, 일반적으로 크레킹을 무력화 시키는데는 크게 영향을 미치지는 않는다. 보안 전문가와 크래킹 소프트웨어 제작사들은 1초에 수십 조의 해시 알고리즘을 위한 해시 생성 속도를 요구한다. 수천대의 기계에서 초당 각기 1조의 해시를 생성하는 것은 한 달에 약 $2.6* 10^{10}$개의 해시 생성에 해당한다.

경우에 따라서 패스워드 해시가 위협이 되는 곳에서는 각 조직이 패스워드의 만기, 길이, 복잡도에 대한 정책을 설정 할 때 고려해야 하는 것으로 크레킹 능력을 추정해야한다. <표 3-1>에 나타낸 키 공간을 고려 할 때 문자 집합크기가 72이고 8자 길이의 패스워드는 최대 $7*10^{14}$ 개의 키 공간을 가진다. 앞서 언급한 예에서 전체 키 공간을 위한 해시는 12분 안에 생성 될 수 있다. 문자 집합 크기가 95로 증가시키면 2시간까지 그 시간이 증가한다. 그러나 12자 길이로 증가시키고 문자집합 크기를 72자로 하면 모든 해시를 생성하는데 필요한 시간은 500년까지 증가하게 된다.

설팅의 사용은 크레킹을 더욱 어렵게 한다. 예를 들면 48비트의 설팅

값 사용은 원시 패스워드 해시에 48비트 패스워드 해시를 추가하게 된다. 따라서 설팅된 패스워드는 크레킹 하는데 시간소모를 많이 하게 한다. 따라서 패스워드 만기, 길이, 복잡도에 관한 정책은 설팅의 사용을 고려해야한다.

몇 년을 계산하여 모든 해시가 생성되는 경우에 패스워드 만기는 크레킹을 완화시키는데 별 영향을 미치지 않을 수도 있다. 일반적으로 패스워드 만료기간은 크레킹을 완화시키는데 크게 도움을 주지는 않는다.

3) 사회 공학적 공격

공격자는 사회 공학적 기법을 사용하여 공격자 선택 패스워드로 기존의 패스워드를 변경하는 속임수를 사용 할 수 도 있다.

4. 노출(손상)된 패스워드 사용

공격자가 추측, 크레킹, 탈취 등으로 패스워드를 획득했다면 공격자는 사용자가 변경 할 때까지 그 패스워드를 사용 할 것이다. 그와 같은 패스워드 사용의 잠재적 영향을 감소시키기 위해서 각 조직은 패스워드가 일정 기간 지난 후에는 신규 패스워드를 사용하도록 패스워드 만기 메커니즘을 구현하고 있다. 이 방법이 패스워드 누출 영향을 감소시키는 장점이 있지만 어떤 경우에는 효과성이 없다. 예를 들면 공격자가 과거 패스워드와 같은 방법(사용자 컴퓨터의 키 로거 등을 수행)으로 신규 패스워드를 알아냈을 때, 공격자가 백 도어 같은 것을 설정하여 패스워드 없이 접근하는 방법이 있을 때는 효과가 없다. 패스워드 만기는 사용자에게 가끔 일정기간마다 신규 패스워드를 생성하고 기억해야 한다는 불만을 야기 시킨다.

각 조직들은 보안의 필요성과 사용편의성에 대한 균형을 토대로 패

스워드 만기 메커니즘을 사용 할 것인지와 만기 기간을 얼마로 설정 할 것인지를 결정해야 한다. 만일 그 조직이 사용자 패스워드의 안전 보관을 제공한다면 사용자들은 패스워드를 기억 할 필요가 없고, 패스워드 만기는 사용자에게 불편을 덜 주게 된다. 패스워드 해시에 대한 비 입증 접근을 포함한 위협이 있는 경우에는 해시로부터 패스워드를 크렉하는 요구 시간보다 더 짧은 패스워드 만기 시간을 갖도록 설정해야한다. 또 다른 고려사항으로는 인증의 빈도이다. 어플리케이션에 단지 1년에 몇 번 정도 접근하고 패스워드 만기정책이 시행된다면, 그 패스워드는 사용자가 인증을 시도 할 때마다 매번 만료 될 것이다. 조직이 패스워드 만기 요구사항을 선택하는데 고려해야하는 또 다른 요소는 패스워드 저장소의 강도, 전송 알고리즘과 시스템 보안 요구사항을 포함하는 것이다. 각 조직은 시스템, OS, 어플리케이션의 형태에 따라 패스워드만기 정책을 다양하게 할 필요가 있다. 즉 보안의 필요성과 사용편의성 요구사항을 반영하는 것이다.

패스워드 만기가 적용 될 때 사용자가 자신의 패스워드를 기억할 것으로 기대한다. 즉 사용자가 곧 패스워드가 만료 될 것이라는 알려 적어도 며칠 동안 기억하기 좋은 패스워드이면서 강도 높은 것을 선택하도록 지원해야한다. 보통 이런 안내를 하지 않으면 급하게 패스워드를 변경 할 때 덜 복잡하고 단순히 기억하기 쉬운 패스워드를 선택하게 된다. 신규 패스워드 설정에서 사용자는 물리적으로 조직의 내부에 위치하지만 출장 등으로 원격에서 작업하는 경우가 있다면, 적어도 패스워드 기간 만료 1, 2주일 전에 사용자에게 공지해야 한다. 이는 사용자가 출장지에서 원격 작업을 하기 이전에 패스워드를 설정하게 해주기 때문이다. 패스워드 만기는 사용자가 이전에 사용한 패스워드와 다른 것을 선택하지 않는다면 효과가 없다.

패스워드 히스토리는 신규 패스워드나 패스워드 해시를 비교하기위해 이전에 사용한 패스워드나 해시를 보관하는 기능이다. 신규 패스워

드는 히스토리를 통하여 검사 된다. 이전 패스워드 수나 그 보관기간은 정의되어야 한다. 패스워드 히스토리와 관련한 패스워드 속성은 최소 패스워드 나이다. 패스워드 나이는 패스워드 변경 마다 필요한 소요되는 총 시간을 말한다. 패스워드를 기억하는데 요구되는 노력을 감소시키기 위해서 사용자는 패스워드 히스토리 보관 버퍼를 초과하도록 패스워드를 주기화 할 수 있으며, 일정 주기가 경과되면 초창기에 사용한 패스워드를 사용 할 수 있다. 최소 패스워드 나이가 이러한 사용을 방해하지만 저지하지는 못한다. 어떤 패스워드 히스토리 메커니즘은 이전 패스워드와 완전히 다르지 않음을 구별 할 수 있다. 신규 패스워드 선택 시 어떤 사용자는 과거 패스워드를 변화시켜 사용하려는 경향(예 : "password07"을 "password08"으로)이 있다. 이것은 과거 패스워드를 알고 있는 공격자에게는 쉽게 노출 될 수 있다. 어떤 패스워드 히스토리 메커니즘은 이전 패스워드와 일정 수의 같은 글자와 공통인 경우에 거부하도록 구성되어 있다. 그러한 기능이 없으면 사용자는 자신의 패스워드에 숫자만을 변경하기가 쉽다. 이것은 패스워드 만기를 무용지물로 만들고 취약한 패스워드를 만드는 원인이 된다.

패스워드 히스토리 메커니즘은 일반적으로 단일 인증 메커니즘으로 동작하며, 여러 메커니즘으로 히스토리를 검사 할 수 없다. 이것은 사용자가 여러 시스템에 같은 패스워드 사용이 가능함을 의미한다. 사용자는 자주 이와 같이 사용하여 기억해야 할 패스워드 수를 줄이지만 공격자가 하나의 패스워드만을 획득하여도 조직에 위험을 증가 시키게 한다. 더구나 관리자는 가끔 개인 워크 스테이션상의 로컬 사용자 계정과 중앙 집중화된 관리자 권한을 가지는 도메인 계정에 패스워드를 재사용하는 경우도 있다. 중앙 집중화된 패스워드관리의 보안이 개인 워크스테이션보다 높기 때문에 더 큰 위험을 가지게 된다. 워크스테이션을 공격하여 정보를 얻은 자는 도메인 관리자를 크렉하여 기업의 자원에 접근할 수 있다.

내 외부 시스템이 결합된 시스템을 통과하는 패스워드 재사용을 검출하기 쉬운 방법은 없다. 패스워드 재사용 가능성을 감소시키기 위해서 각 조직은 자신의 IT 시스템과 외부 시스템과 밀접한 관련을 갖는 패스워드 사용을 금지 시키는 패스워드 관리 정책을 수립 할 수 있다. 패스워드 관리 정책은 사용자 혹은 로컬 계정에서 중앙 집중식 관리 수준의 패스워드 재사용을 명백하게 금지할 수 있다. 패스워드 재사용의 위험성을 설명하고 패스워드 관리와 보호의 중요성을 강조하는 적정한 사용자 훈련이 있어야 한다. 패스워드 재사용여부를 감독하는 메커니즘 없이 재사용관한 정책만으로 여러 패스워드를 기억 할 필요가 있는 사용자가 재사용을 감소시키기에는 한계가 있다.

패스워드 관리 시스템이나 패스워드 관련 다른 자원이 위태롭게 되었다고 생각되면 각 조직은 신속하게 위태로운 약점을 해소하는 조치를 취하고, 즉시 모든 사용자에게 패스워드 변경을 요구하고, 위태로운 시스템을 안전한 상태로 회복시켜야 한다. 기업 패스워드 변경 구현은 주의 깊은 계획과 협력을 요구한다. 절차들이 모든 사용자들에게 공지되어야한다. 이 공지는 단순히 사용자에게 패스워드가 즉시 변경 될 필요가 있다는 내용을 알리는 것이다. 사용자들은 패스워드 변경에 대한 교육을 받아야한다. 패스워드가 사전에 배정된 패스워드로 설정되어 있으면 사용자가 안전한 방법으로 배정된 패스워드를 사용하는 절차가 있어야 한다.

Ⅳ. 패스워드 관리 제품

많은 조직들은 사용자가 기억할 패스워드와 계정 수를 감소시키기 위한 범 조직 패스워드관리 제품을 설치하고 있다. 로컬 패스워드관리 유틸리티가 패스워드 스토리지에 사용 될 수 있다. 전체와 부분 패스워

드 관리 제품들은 사용자와 패스워드변경과 설정에 관련한 지원창구의 부담을 줄일 수 있다. 패스워드관리 제품들은 패스워드가 노출될 가능성을 줄여준다. 여기에서는 두 가지 형태의 중앙집중식 패스워드 관리 제품에 대하여 고찰한다. 즉 SSO(single sign-on)과 패스워드 동기화에 대하여 사용상 특징을 중심으로 이들 기술의 간단한 비교를 하고자 한다.

1. SSO 기술

SSO기술은 사용자가 사용하고자하는 모든 자원에 접근하기위해서 1회 인증만을 허용한다. 개별 자원에 대한 인증은 SSO기술에 의해 수행된다. 많은 인증방법들이 SSO에 의해 지원되지만 여기에서는 패스워드 기반 인증만 언급한다. 일반적으로 SSO는 유일하고 강력한 사용자 패스워드를 생성한다. 보통 끝단 사용자는 어떤 종류의 자원 패스워드도 알지 못한다. 왜냐하면 각기 다른 패스워드가 각 자원에 사용되기 때문에 사용자는 패스워드를 기억 할 필요가 없으며, SSO는 각 자원이 빈번하게 패스워드를 변경하는 것만큼의 강력한 각기 다른 패스워드를 생성 할 수 있다.

모든 환경에서 모든 시스템과 자원에 대하여 SSO 제품이 인증을 실행하지는 않으며, 대부분의 SSO 제품은 몇몇 시스템과 자원에 대하여만 인증을 실행 할 수 있는데, 이를 RSO(reduced sign-on)라 한다. 제한된 RSO 기능을 제공하더라도 SSO기술은 사용자가 매 인증 할 때마다 기억 할 필요가 있는 사용자이름과 패스워드의 수를 감소시키는데 매우 효과적 일 수 있다.

SSO 기술에는 여러 가능한 구조가 있다. 일반적 구조는 SSO 사용자 인증을 위한 Kerberos같은 인증서비스와 SSO가 인증할 자원에 대한 인증정보를 저장하는 LDAP(Lightweight Directory Access

Protocol) 같은 데이터베이스나 디렉토리 서비스를 갖는 것이다. 정확한 구조와 관계없이 SSO 제품은 보통 많은 사용자를 위한 인증서를 보유하는 하나 혹은 그 이상의 중앙집중식 서버를 포함한다.

이런 서버는 많은 자원에 대한 인증시 실패의 원인이 되기도 한다. 즉 서버의 가용성이 모든 자원의 가용성에 영향을 미치게 되는데, 이는 인증서비스를 위한 서버에 의존하기 때문이다. 또한 서버의 위태로움은 많은 자원의 인증서를 위태롭게 할 수 있다. 또한 SSO기술 자체에 대한 사용자 인증은 매우 중요하다. 적절한 상호 인증이 수행되지 않는다면, SSO 기술은 MITM (man-in-the-middle) 공격에 취약 할 수 있다.

패스워드 같은 민감한 인증정보의 모든 통신은 승인된 암호기술을 사용하여 무결성과 기밀성이 보장 되어야 한다. 재연공격(Replay attacks)은 인증서와 관련이 있어, 재연공격을 방해할 타임스탬프나 기타 다른 메커니즘이 인증서 전송시 포함 되어야한다. SSO 사용자 인증과 관련하여 또 다른 중요사항은 SSO 패스워드가 사회 공학적 방법, 피싱, 키 로깅 등을 통하여 위태로울 수 있다는 것이다.

2. 패스워드 동기화

패스워드 동기화(password synchronization) 제품은 사용자로부터 패스워드를 취하여 그 패스워드로 다른 자원에 대한 패스워드로 변경한다. 그 후 사용자는 그 패스워드를 사용하여 각 자원을 직접 인증한다. 거기에는 그 자원에 대한 인증을 수행하는 디렉토리나 인증 서버가 없다. 패스워드 동기화의 주요 장점은 사용자가 기억해야 할 패스워드의 수를 감소시키는 것으로, 사용자에게 강력한 패스워드 선택과 좀더 쉽게 기억하도록 허용하는 것이다. SSO기술과 달리 패스워드 동기화는 사용자가 인증에 필요한 횟수를 감소시키지는 않는다.

패스워드 동기화 제품은 일반적으로 SSO 기술보다 구현하기가 쉽고 저렴하지만 중대한 보안 단점을 가지고 있다. 패스워드 동기화는 여러 자원에 동일한 패스워드를 사용하기 때문에 각 자원마다 패스워드나 패스워드 해시를 보관하고 있으며, 단 하나의 패스워드가 위태롭게 되면 모두에 여향을 준다. 특히 특별한 보안 요구사항이 필요한 자원에 패스워드 동기화를 사용하는 것은 치명적이다. 예를 들면 저수준 보안을 요하는 자원의 패스워드와 고수준의 보안을 요하는 자원의 패스워드 동기화를 적용하는 것은 문제가 된다. 이는 공격자가 저수준의 자원을 공격하여 고 수준의 보안 자원에 접근이 가능하기 때문이다.

또 다른 패스워드 동기화와 관련한 중요 문제는 패스워드의 강도로 최저 공통분모가 적용 된다는 것이다. 동기화가 10개 시스템에 사용된다고 가정 할 때, 이들 시스템 중 두 개는 특수문자를 지원하지 않고, 하나의 시스템은 패스워드길이를 6-8자만 지원하면 이들 자원에 대한 패스워드 동기화는 특수문자가 없는 6-8자 패스워드를 가지게 될 것이다. 이 결과는 각 개별 시스템에서 지원하는 것보다 패스워드 강도가 하락 할 것이다. 또한 패스워드가 동기화되지 않을 수도 있다. 예를 들면 사용자는 패스워드 동기화 사용자 인터페이스 대신에 해당 자원에 직접 패스워드를 변경 시킬 수도 있다. 이것은 나머지 것과 다른 패스워드를 갖게 되는 것이며, 향후 관련 자원의 동기화 실패의 원인이 될 수도 있다. 또한 백업을 통한 복구시에도 과거의 특정 자원에 대한 패스워드 때문에 변경을 해야 하는 문제가 남게 된다.

3. 로컬 패스워드 관리

패스워드관리의 또 다른 접근이 로컬 패스워드 관리 소프트웨어이다. 패스워드 관리 소프트웨어는 사용자에게 사용자이름, 패스워드와 계정번호 같은 기타 민감 정보의 일부를 저장하도록 허용하는 유틸리티이

다. 패스워드관리 소프트웨어는 사용자가 기억해야하는 패스워드수를 경감시킬 수 있다. 패스워드 관리 소프트웨어 자체가 마스터 패스워드를 가지고 있어, 이 패스워드를 소프트웨어에 의해 저장된 패스워드를 얻기 위해 입력한다. 마스터 패스워드는 저장된 사용자의 패스워드들을 보호하게 되며, 사용자는 이 패스워드만을 기억하면 된다. 어떤 패스워드 관리 소프트웨어 유틸리티는 사용자가 로컬 컴퓨터 대신에 이동식 매체(USB 등)에 패스워드 저장을 허용하며, 이는 필요시 컴퓨터에 연결하고, 분리하여 저장함으로서 보안성 강화를 제공한다.

대부분의 패스워드 관리 소프트웨어 유틸리티에서 사용자는 해당 패스워드를 복사하여 사용 할 수 있도록 목록으로부터 계정을 선택하고, 해당 패스워드를 복사하여 붙이기 작업으로 입력한다. 좀 더 자동화된 유틸리티는 자동적으로 계정을 선택하면 해당 패스워드가 입력되는 형태를 취하기도 한다.

패스워드 관리 소프트웨어를 사용 할 때 반영해야 되는 사항은 다음과 같다.

① 소프트웨어 타임아웃 설정하기 : 일정 시간이 경과되면 자동적으로 패스워드를 동결시킨다.
② 패스워드의 복사/붙이기 작업 후에 지우기 : 많은 소프트웨어는 자동적으로 이를 수행 한다
③ 정기적으로 패스워드 데이터베이스 백업하기 : 특히 패스워드가 변경된 후.
④ 쉽게 추측되거나 크레킹 되지 않게 강력한 마스터 패스워드 사용하기

패스워드 관리 소프트웨어는 승인된 알고리즘으로 구현하고 저장된 패스워드의 기밀성을 보호해야한다. 패스워드 관리 소프트웨어가 패스워드의 모든 위협을 제거 할 수 없다. 예를 들면 컴퓨터가 악성 코드, 키 로거, 기타 악의적 요소 등으로 위태롭게 되면, 공격자는 패스워드

관리시스템에 접근하여 패스워드를 탈취 할 수 있다. 부가적으로 패스워드관리 어플리케이션 또한 약점을 상속받을 수 있다. 사용자는 패스워드가 변경 될 때마다 패스워드 데이터베이스를 수동으로 업데이트 해야만 한다.

어플리케이션에 패스워드 생성 기능이 있으면 각 계정에서 요구하는 특정 패스워드 강도를 만족하는지 패스워드를 사용 할 때 마다 조정할 필요가 있다. 이때 사용자가 패스워드 강도를 더 낮추어 조정 할 위험성이 크기 때문에 주의 할 필요가 있다. 마지막으로 어떤 패스워드 관리 어플리케이션은 중앙집중식으로 관리되지 않음으로서 사용자가 어플리케이션의 구성을 부적절하게 할 수도 있다. 이것은 장기간 패스워드가 암호화 되지 않은 상태로 캐시에 남아 있거나 저장되는 결과를 초래 할 수 있다. 패스워드 관리 소프트웨어가 중앙집중식으로 관리 되지 않을 경우에는 각 조직들은 패스워드 정책에 규정을 두어 정기적으로 이를 검사하여 정책 요구사항을 만족시켜야 한다.

웹 브라우저 같은 어플리케이션은 기본적으로 패스워드를 입력 할 때 패스워드 관리 속성(패스워드 자동 로그인 기능)을 제공하고 있다. 몇몇 어플리케이션들은 기본적으로 내장된 패스워드관리 유틸리티를 제공 하고 있어, 사용자 설정 마스터 패스워드를 통하여 접근을 통제하고 안전하게 패스워드를 저장하고 있지만, 어떤 경우에는 저장된 패스워드가 안전하지 않은 상태로 저장될 수도 있다. 따라서 각 조직은 패스워드 관리 소프트웨어에서 패스워드를 저장하는데 따른 위험을 충분히 고려해야한다.

4. 패스워드 관리 기술의 비교

<표 4-1>은 패스워드 관리 기술의 세 가지 형태를 비교한 것이다. 비교의 초점은 기술이 실패하거나 패스워드가 위험 해진다면 사용자와

조직에 어떻게 영향을 미치는지와 패스워드 관리기술의 유용성이다.

<표 4-1> 패스워드 관리 기술의 유용성 비교

	SSO와 RSO	패스워드 동기화	로컬 패스워드관리 소프트웨어
사용자가 기억해야 되는 패스워드 수가 많은가?	예	예	예
부가적인 과정 없이 사용자가 인증 할 수 있는가?	예	예	아니오
사용자가 수행해야 할 인증수가 많이 감소 되는가?	예	아니오	아니오
패스워드 관리기술이 일시적으로 중단되면 사용자가 크게 영향을 받지 않는가?	아니오	예	아니오
개별자원에 대한 사용자 패스워드의 영향이 각 자원에 제한되어 취약해 지는가?	예	아니오	사용자가 각 자원에 유일한 패스워드를 사용한다면 "예"

조직에 구축할 패스워드 관리 기술을 선택 할 때 표 4-1에 나타낸 특성을 유용성 요구사항과 어떻게 비교 할 것인지 주의 깊게 고려 할 필요가 있다. 만일 패스워드 관리 기술이 조직의 유용성 요구사항을 충족시키지 못하게 구축 된다면, 사용자는 로컬 패스워드 관리 소프트웨어 패스워드를 저장하는 대신에 종이에 기록하는 등 그 기술을 우회할 수도 있다. 또한 각 조직은 패스워드 관리 기술 자체에 대한 보안을 고려해야한다. 또 다른 중요 요소는 사용자가 패스워드 관리 기술을 인증하는 방법 이다. 만일 인증의 형식이 패스워드라면, 이들 패스워드중 하나가 위험에 노출되면 패스워드 관리 기술에 저장되어 있는 다른 모든 사용자의 패스워드가 위험에 노출되게 된다.

또한 각 조직들은 패스워드 관리 기술에 저장된 패스워드와 관련한 피해가 발생하면 미치는 영향정도를 고려해야한다. 기술이 저수준의 패스워드를 지원하도록 설치되고 그 기술의 안전대책이 그 수준에 적합하게 설계되어 있다면, 고 수준의 영향을 미치는 패스워드를 저장하는 것은 큰 문제가 된다. 어떤 경우에는 좀 더 높은 수준의 영향을 미치는 패스워드를 위해서 분리된 패스워드 관리기술을 설치 할 수 한다. 이것은 각 자원에 같은 패스워드를 사용하는 패스워드 동기화 제품에서 특히 중요하다. 자원들이 다양한 보안 수준(낮음, 중간, 높음)이라면, 공격자는 중간수준의 영향을 미치는 시스템보다 강도측면에서 덜 안전한 저 수준 영향 시스템을 공격하여 사용자 패스워드에 접근 할 수 있다. 사용자 패스워드가 각 자원에 동기화 되어 있기 때문에 낮은 수준의 영향을 미치는 시스템에 접근하여 중간 이상의 수준 시스템에 사용 될 수 있다. 각 조직은 다양한 영향을 가지는 시스템에 패스워드 동기화를 적용 할 때 공격자가 고 수준의 영향을 미치는 시스템에 접근 할 수 없다는 보증을 할 수 있어야한다.

V. 결론

본고는 미국 연방 정부에서 권고하고 있는 패스워드관리에 대하여 서술하였다. 현재 컴퓨터 시스템을 이용한 사회생활이 보편화 되면서 각 개인과 조직은 많은 컴퓨터 시스템을 구축 운영하고 있다. PC수준의 컴퓨터에서부터 조직의 행정업무, 관리업무, 생산업무, 통제업무, 생활정보 제공 및 활용에 이르기까지 그 범위와 기능이 매우 다양하다. 따라서 각 개인이 접속해야하는 컴퓨터 시스템과 어플리케이션은 그 수가 급격하게 증가하고 있다. 컴퓨터에 접속하기 위해서는 사용자 ID와 패스워드가 보편적으로 사용되고 있다.

패스워드에는 여러 가지 위협이 있으며, 이들 위협의 대부분은 부분적으로 경감 시킬 수 있다. 또한 사용자는 많은 패스워드를 관리해야 하고 기억해야하는 부담을 갖게 된다.

그러나 조직 패스워드 관리 메커니즘이 이와 같은 부담을 경감시킨다 해도 사용자는 사용상 단점을 가지며, 심각한 보안 사고를 발생 시킬 수 있다.

본 서술에서는 패스워드 관리의 필요성과 아울러 패스워드에 대한 위협으로 패스워드 탈취, 패스워드 추측과 크래킹, 패스워드 변경, 노출된 패스워드의 사용에 따른 각 종류별 위협 요소와 완화 방법에 대한 권고를 정리하였다. 또한 패스워드 관리 제품을 두 가지 기술(SSO, 패스워드 동기화)을 중심으로 비교 서술 하였다.

참고문헌

http://www.elcomsoft.com/edpr.html?r1=pr&r2=multi-gpu.

C. Kuo, S. Romanosky, and L. F.Cranor, July 2006, "Human Selection of Mnemonic Phrase-based Passwords", Symposium on Usable Privacy and Security, Pittsburgh, PA,

NIST SP 800-53 Revision 2, "Recommended Security Controls for Federal Information Systems"

FIPS 199, "Standards for Security Categorization of Federal Information Systems"

NIST SP 800-63 Revision 1, "Electronic Authentication Guideline"

Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

Office of Management and Budget (OMB) Circular A-130, Section 8b (3), "Securing Agency Information Systems,"

NIST SP 800-118, "Guide to Enterprise Password Management"

A Study On Enterprise Password Management Recommendations

Park, Jin-Sub*

Passwords are used in many ways to protect data, systems, and networks. Passwords are also used to protect files and other stored information. In addition, passwords are often used in less visible ways for authentication.

In this article, We provides recommendations for password management, which is the process of defining, implementing, and maintaining password policies throughout an enterprise. Effective password management reduces the risk of compromise of password-based authentication systems. Organizations need to protect the confidentiality, integrity, and availability of passwords so that all authorized users—and no unauthorized users—can use passwords successfully as needed. Integrity and availability should be ensured by typical data security controls, such as using access control lists to prevent attackers from overwriting passwords and having secured backups of password files. Ensuring the confidentiality of passwords is considerably more challenging and involves a number of security controls along with decisions involving the characteristics of the passwords themselves.

* Professor, Dept. of Computer Engineering, Daejeon University

Key words: password management, password policies, data security control, authentication system