효율성과 가용성을 향상시킨 패스워드 관리시스템 연구

서미숙* · 박대우*

*호서대학교 벤처전문대학원

A Study of Password Management System for Improves the Availability and Efficiency

Mi-Suk Seo* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : msseo@smsinfo.co.kr · prof_pdw@naver.com

요 약

발달된 IT 솔루션 기반으로 인한 관리 서버가 증가되고 있고, 서버의 보안성이 중요하다. 효율적인 패스워드를 관리하기 위한 안전한 패스워드 관리시스템에 대한 연구가 필요하다. 본 논문에서는 주기적인 시스템 계정과 패스워드는 숫자와 문자를 섞어 8자리 이상으로 변경을 하는 규칙을 정한다. 또한 각 시스템 계정의 패스워드가 숫자, 영문자, 특수문자를 포함해야 하는 패스워드 셋팅 룰을 정한다. 하지만 새로운 IT시스템의 지속적인 도입과 인력 투입의 한계로 인하여, 안전성을 확보하기 위한 패스워드에 대한 문제가 발생되고 있다. 국내외 통합접근제어 솔루션에서 패스워드 관리 기능을 일부 제공하고 있으나, 고가이고 서버 트래픽에 부하를 주는 단점이 있다. 향후 일반 전산시스템이 융합IT시스템으로 전환이 가속화될 것으로 판단되며, 본 연구에서는 효율적인 패스워드 관리를 위한 패스워드 관리시스템 연구를 통해 가용성과 효율성을 높이면서, 개인정보보호법을 준수할 수 있는 패스워드 관리시스템을 개발한다.

ABSTRACT

By the development of IT, most business has been processed on the IT solution-based servers has increased Therefore, the importance of security of the server is highlighted. And the need for password management server efficient and safe is raised. There is a need to change at least 8 characters to mix the numbers and letters and password change passwords on a regular basis, you need a password for each system account is set in a different way, but the continuation of the system there is a tendency to password problems occur problems caused by the limits of the introduction of human resources and introduction basis occurs. The password management feature, though it is expensive is partially providing integrated access control solutions at home and abroad, there is a drawback that stresses the traffic on the server. Future, we conducted a study of password management solutions for the server of the server is determined IT transformation trend of non-IT field to accelerate, is continuously increasing it accordingly

키워드

Password, Password Management, Solution, Security

Ⅰ. 서 론

IT의 발달로 인하여 대부분의 업무가 IT 솔루션 기반 위에 처리되고 있으며 이를 위한 서버가 증가되고 있고 서버보안의 중요성이 강조되고 있다. 서버가 늘어나고 외부 지원인력의 증가로 인하여 효율적이고 안전한 서버 패스워드 관리 필요성이 제기되고 있다. 또한 “개인정보보호법” 제5조에서는 개인정보 취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다는

내용의 비밀번호 관리에 대한 기준을 고시하고 있다[1].

주기적인 시스템 계정 패스워드 변경과 패스워드는 숫자와 문자를 섞어 8자리 이상으로 변경을 해야 하며 각 시스템 계정의 패스워드가 다르게 설정이 되어있어야 한다. 하지만 시스템의 지속적인 도입과 인력 투입의 한계로 인한 어려움이 발생하여 패스워드에 대한 문제가 발생되는 추세이다. 패스워드의 수가 많아지고 이에 따라 당연히 잊어버리게 되는 패스워드들도 많아지게 된다. 패스워드의 수가 5개에서 10개를 모두 한꺼번에 기억하는 것은 어려운 일다. 패스워드의 수가 많아지게 되면서 이에 대한 해결책 제시를 위해 고민해 왔으며 또한 시스템의 ID 도용을 통한 불법적인 OS 및 어플리케이션 접속 사례로 내부 어플리케이션 ID, Password 관리 강화 및 관리기능 서비스 필요성이 대두되고 있다.[2]

따라서 개별 조직 내에 존재하는 다수의 서비스들에 대한 사용자들의 패스워드를 효과적으로 관리할 수 있는 방법의 연구가 필요하다.

II. 관련연구

2.1 일반적인 패스워드 관리

2012년 10월 Webroot 라는 국제 정보보호 회사의 2,500명 이상의 사람들을 대상으로 수행한 조사에 따르면[3] 패스워드 사용에 관하여 사람들은 다음과 같은 행위를 보이고 있다.

○51% 이상의 사람들이 때때로 패스워드를 기억하지 못하는 경우가 있다.

○30%의 사람들이 패스워드를 기록하여 책상 서랍 등의 장소에 놓고 사용한다.

○62%의 사용자들이 자신의 Facebook 패스워드를 한번도 바꾸지 않고 있으며, 약 10%의 사람들이 자신의 인터넷 뱅킹 소프트웨어의 패스워드를 한번도 바꾼 적이 없다.

이러한 패스워드 사용에서의 비보안성은 다양한 정보시스템을 사용하는 시스템에서는 보안상의 취약점이 될 수 있으며, 정보시스템 내에 가치있는 정보를 관리하는 조직에서는 이를 관리할 수 있는 방법이 제공되어야 한다.

조직 내에서 가장 큰 보안 위험요인은 내부로부터의 위협이며 보안사고의 86%는 시스템의 최고 권한을 갖는 사람들에게 발생하고 그중 사고 발생 원인의 50%는 최고 관리자 권한의 체계적인 관리부재로 인한 보안사고가 대다수 이다.

2.2 패스워드 관리 방법

IT정보보안은 아무리 강조해도 지나치지 않을 정도로, 관심을 갖고 신경을 쓰야 한다.

그러나 이용자의 입장에서는 패스워드 기억하기도 어렵고 입력하기도 힘들다. 인터넷 이용자들은 평균25개의 온라인 계정을 갖고 있다고 한다.

패스워드를 생성시 좀더 안전한지 여부를 확인하기 위하여 https://howsecureismypassword.net 에서 패스워드 안전검사 할 수 있다.

일반적으로 패스워드를 안전하게 관리하는 법과 패스워드 생성법은 다음과 같다.

○첫째로 본인의 영문이름이나 주민번호 뒤 숫자 4자리등 내 주민번호를 알고 있는 사람이 유추가능한 조합은 피한다.

○둘째, 인터넷 회원가입시 주민번호를 되도록 사용하지 말고 아이핀과 같은 대체 인증수단을 사용한다.

○셋째, 패스워드를 주기적으로 변경하고 PC에 기록보관하지 않는다.

○넷째, 문자와 숫자, 특수기호가 조합된 패스워드를 만들어 사용한다.

○다섯째, PC방 같은 곳에서는 되도록 메일서비스등에 로그인하지 말고, 퇴실할때는 인터넷로그 삭제나 열어본 페이지등을 꼭 삭제

○여섯째, 패스워드는 최소 8~10자 이상의 길이로 만들어라

마지막으로 P2P사이트나 공개된 자료를 다운로드 받을 때 무작정 실행하지 말고 바이러스 검사를 한 뒤 실행하는 것이 좋다.

2.3 패스워드 자동 변경 및 관리

개별 조직 내에 존재하는 다수의 서비스들에 대한 사용자들의 패스워드 관리를 효과적으로 할 수 있는 방법은 접근을 원하는 사용자에게 실시간으로 원타임 패스워드를 제공하는 기술・솔루션 내의 패스워든 암호화되어 존재하고 그 외에 패스워드는 주기적, 임시적 갱신 및 관리자 통지 기능 등 패스워드 관리를 위한 효율적인 방법이 있다.

이와 같은 방법을 활용하였을 때 다음과 같은 기대효과가 있다.

○ 기관내 시스템의 보안성 증가: 사용자들의 단일 패스워드 사용 기간 등을 감시하여 패스워드 갱신 주기를 단축시킬 수 있다. 또한 패스워드 분실의 가능성이 상당히 감소하므로, 긴 패스워드를 사용할 수 있다. 또한 다수의 패스워드 관리를 위해 패스워드들을 자신의 책상 위에 적어 놓는 등의 시스템 외적인 보안 취약점을 발생시킬 여지가 줄어들게 된다. 최종적으로 패스워드 사용으로 인한 보안성 효과가 증대됨. 또한 관리자 패스워드도 특별한 관리 (패스워드 미갱신시 이메일을 통한 알림 및 강제 갱신 등) 가 가능하므로 패스워드 관리 취약으로 인한 보안상의 취약점이 감소하게 되는 장점이 있다.

○ 패스워드 사용시 발생하는 사용자들의 불편함 감소: 패스워드 사용시 불필요하게 다른 곳에 기록할 필요가 없으며, 분실시에도 자동으로 알려주는 기능이 존재한다. 또한 자동으로 패스워드를 갱신해 주므로 패스워드 사용으로 인한 불편함이 감소된다.

III. 패스워드 관리시스템 동작과정 및 구조

다양한 서비스의 관리자 패스워드를 통합하여 관리 할 수 있도록 하며, 개별 서비스에 Agent설치 없이 솔루션으로의 아이디/패스워드 초기등록으로 패스워드 설정, 패스워드 최종갱신 시간 관리 및 Linux(특정버전), Windows Server 2000~2008, MySQL, MS-SQL, Oracle등 다수의 서비스에 대한 패스워드의 통합 관리가 가능하도록 한다. 전체 시스템의 동작과정 및 구조를 요약한 내용을 아래의 그림과 같이 기술한다.

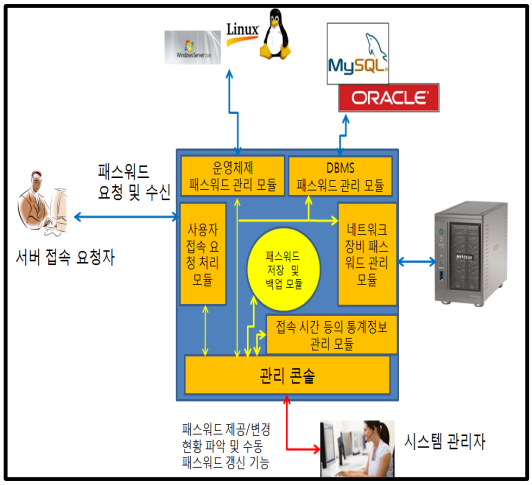

그림 1. 시스템 구성도

IV. 패스워드 인증구조 및 계정관리

4.1 윈도우의 계정관리 인증 구조

식별(ID. 중복불가), 인증(Aulthentication=패스워드.. 중복가능), 식별과 인증이 맞으면 권한(Authorization)을 부여

Winlogon(winlogon.exe):유저모드. 윈도우 로그인 프로세스의 한 부분

GI"NNA(msGINA.dll);winlogon내에서 msGINA.dll을 로딩시켜 사용자가 입력한 계정과 패스어드를 LSA에게 전달한다. LSA(Local Security, lsass.exe) : 유저모드. 전달받은 계정과 암호를 검증하기 위해 NTLM모듈(해쉬 알고리즘)을 로딩하고 패스워드를 해쉬화해서 SAM의 DB에 있는 해쉬갑과 대조해서 일치하는지 확인. SRM이 작성한 감사로그를 기록하는 역할

SAM(Security Account Manager) : 사용자/그룹 계정 정보의 데이터베이스 관리, 사용자 로그인 정보와 SAM 데이터베이스 정보를 비교 " 인증여부 결정, %system%/system32/config/sam (접근은 관리자만)

SRM(Security Reference Monitor): SAM이 사용자의 계정과 패스워드가 일치하는 지를 확인하여 SRM에게 알려주면 SRM은 사용자에게 고유의 SID를 부여한다. 그림 2.와 같이 윈도우의 계정관리 인증구조를 확인할 수 있다.

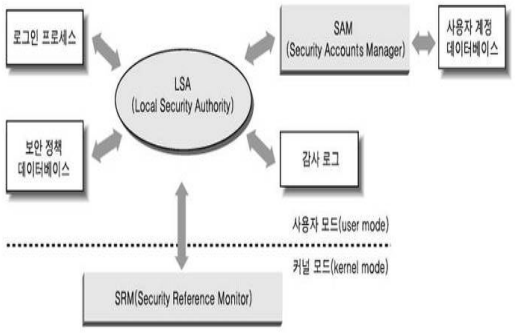

그림 2. 윈도우 계정관리 인증구조

윈도우의 인증방식

· LM(LAN Mangaer) - 보안에 가장 취약.

윈도우에서 가장 약한 인증방법, 랜에서 파일을 공유하기 위해서 사용하는 인증방법으로 보통 윈도우 95, 98, Me 버전에서 사용.

LM을 이용한 공유 파일 패스워드 설정은 아무리 복잡하더라도 크랙하는데 10여초 이상 소요되지 않음.

· NTLM 버전1 : LM보다는 안전하지만 취약점이 발견되어 오래 적용되지는 않았다. 인증에 도전/응답 방식을 사용

· NTLM 버전2 : 윈도우 XP와 2000의 시스템에 적용.

4.2 리눅스/유닉스 인증구조

리눅스와 유닉스의 인증구조는 /.etc/passwd, /etc/shadow이다.

/etc/passwd : 이 파일은 644 권한으로 일반 계정의 권한으로도 패스워드파일을 읽을 수 있다. 따라서 시스템에 존재하는 계정의 확인이 싶다.

passwd 파일구조

```
root : x : 0 : 0 : root : /root : /bin/bash
①  ②  ③  ④   ⑤     ⑥        ⑦
```

① 사용자계정

② 암호화된 패스워드

③ 사용자번호: 관리자 0번, 일반사용자 500번부터의 번호

④ 그룹ID : 관리자 그룹이므로 0번임

⑤ 실제 이름, 시스템 설정에 영향이 없고 자신의 이름을 입력할 수 있다.

⑥ 사용자의 홈 디렉토리를 설정 : 관리자 홈디렉토리가/root이다.

⑦ 사용자의 셸을 정의한다.

shadow 파일구조

각 필드의 구분자는 콜론(:)이며, 각 필드는 아래의 의미를 가지고 있다.

Login Name : 사용자 계정

Encrypted : 패스워드를 암호화시킨 값

Last Changed : 1970년부터 1월 1일부터 패스워드가 수정된 날짜의 일수를 계산

Minimum : 패스워드가 변경되기 전 최소사용기간(일수)

Maximum : 패스워드 변경 전 최대사용기간(일수)

Warn : 패스워드 사용 만기일 전에 경고 메시지를 제공하는 일수

Inactive : 로그인 접속차단 일 수

Expire : 로그인 사용을 금지하는 일 수 (월/일/연도)

Reserved : 사용되지 않음

패스워드를 암호화할때는 앞부분 Fz4q1GjE 부분이 salt 값인데 이 salt 값을 이용해서 암호화를 하게 된다.

IV. 결론

우리 기업들의 IT환경에서 시스템에 접속하는 패스워드를 주기적으로 변경한다는 것은 현실적으로 매우 어렵다. 시스템의 종류도 다양하고 관리자 또한 현실적으로 부족하다. 하여 외부 용역업체나 유지보수 업체의 유지보수시 마다 동일한 패스워드를 알려 주는 경우가 많았다. 뿐만 아니라 여러 시스템의 패스워드 관리가 어려워 메모지나 대장에 수기로 기입하여 장부형태로 보관하는 경우도 많다. 이는 보안적인 측면에서 볼 때 매우 위험한 방법이다.

본 논문에서는 이러한 문제를 해결하기 위해 관리자의 패스워드를 효율적으로 관리 하기위해 리눅스와 유닉스, 윈도우의 인증구조 방법을 제시한다.

향후 연구로는 안전하게 패스워드를 전송하는 방법과 다양한 종류의 패스워드 서비스을 위한 연구가 필요하다.

참고문헌

[1] 행정안전부, “개인정보의 안전성 확보조치 기준 및 해설서”, 2011년 9월

[2] jong-I1 Baek, "A Study on Security Management Technology after Database Vulnerable Object Analysis." International Conference of KiMICS 2011, vol. 4, No 1. pp. 10-13. June 2011.

[3] Webroot "국제정보보호 회사의 설문조사“, 2010년 10월