시스템 접근통제를 위한 패스워드 관리 방안에 대한 연구

백종일* · 박대우*

*호서대학교 벤처전문대학원

A Study of Password Management Methods for System in Access Control

Jong-Il Baek* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : jibaig101@empal.com · prof1@paran.com

요 약

시스템 접근통제를 위한 솔루션은 사용자 개인을 시스템에 인증시키고자 할 때 사용된다. 이러한 유효한 사용자는 과연 바로 권한이 있는 사용자인가 하는 부분으로, 유효한 사용자의 적합성의 여부가 인증되었는지 확실하지 않다는 점이 문제이다. 예를 들어, 한 명의 개발자가 Unix 운영시스템에는 유효할 수 있지만, 권한이 없는 시스템에 대해서는 접근에 제한되어야 한다. 본 논문에서는 1개의 계정으로 여러 사용자가 사용하는 시스템운영의 문제점을 개선하기 위한 세밀한 권한 위임, 세션 감사, 관리자 계정의 정책기반 관리, 모든 권한을 갖는 관리자 계정 배급의 관리와 감사 기능을 통해 시스템 전체적인 접근 제어 방안을 연구한다.

ABSTRACT

System solutions for access control to the user's personal when you want to authenticate to the system is used. The valid user is really just a part of authorized users, the suitability of a valid user has been authenticated are not sure whether the problem is the fact. For example, one developer in the Unix operating system can be valid, but do not have permission to access the system should be limited for. In this paper, a single account for multiple users to use the system operational issues to improve the fine-grained delegation of authority, the session audit, the administrator account's policy-based management, with full rights the administrator account of distribution management and auditing the system overall is the study of access control measures.

키워드

Access Control, Password Management, Security Account, Audit

Ⅰ. 서 론

2011년 9월 30일 시행되는 개인정보보호법은 그간 대책 없이 관리되어 오던 개인정보에 대한 문제점을 개선하기 위해 국가적인 중대사로 인식하여 시행되었다. 이로써 개인정보취급자는 법과 각종 지침을 통해 개인정보 관리방안을 수립하여 개인정보를 보호해야 한다[1].

개인정보보호법과 관련한 지침서 중에서 2011년 9월에 행정안전부에서 발간한 개인정보의 안전성 확보조치 기준 및 해설서는 “개인정보보호법”에 따라 개인정보처리자가 개인정보의 안전성 확보를 위해 이행해야 할 기술적·관리적 보호조치 등의 세부 기준 제시를 목적으로 한다. 본 해설서 제5조에서는 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다는 내용의 비밀번호 관리에 대한 기준을 고시하고 있다[2].

시스템 ID 도용을 통한 불법적인 OS 및 어플리케이션 접속 사례로 인한 내부 어플리케이션 ID, Password 관리 강화 및 관리기능 서비스 필요성이 대두되고 있다[3]. 따라서 1개의 계정으로 여러 사용자가 사용하는 시스템운영의 문제점을 개선하기 위한 세밀한 권한 위임, 세션 감사, 관리자 계정의 정책기반 관리, 모든 권한을 갖는 관리자 계정 배급의 관리와 감사 기능을 통해 시스템

전체적인 접근 제어 방안에 대한 연구가 필요하다.

본 논문은 I장, 서론에서 논문의 필요성을 설명하고, II장, 관련연구에서는 패스워드 운영실태와 관리의 문제점을 정리한다. III장에서는 시스템 접근통제 관리방안을 제시하고, IV장에서는 시스템 접근통제를 위한 패스워드 관리 방안을 연구한다. 마지막으로 V장에서 본 논문의 핵심내용과 향후 연구 방향을 설명한다.

Ⅱ. 관련연구

2.1 농협사태 분석

2.1.1 보안시스템 운영현황

현재 금융기관에 보급되고 있는 모든 보안솔루션들은 소프트웨어 방식으로 개발되어 있어 해커로 인해 보안솔루션들의 취약성이 분석되거나 우회경로가 취득되는 경우 데이터 파괴 공격을 완벽하게 차단하기란 역부족인 것이 현실이다. 농협사태의 경우는 보안솔루션이나 접근통제, 모니터링 시스템으로도 해결할 수 있는 문제가 아니었다. 인공지능 시스템이라 하더라도 ROOT권한에서 내려오는 명령어 (Command)를 정상적인 명령어인지, 비정상적인 명령어인지를 S/W레벨에서 판단하는 데는 분명 한계가 있고, 오로지 삭제명령어를 실행한 ROOT 관리자만이 알 수 있다. 보안기술보다 항상 선행하여 출현하는 신·변종 바이러스나 악성코드로 인해 보안이 뚫리는 최악의 상황에서도 데이터 강제삭제나 파괴 공격을 방지할 수 있도록 하는 사후보안 대책이 필요하다[4].

2.1.2 전산망 운영 실태

모든 전산시스템에서 슈퍼관리자(ROOT) 권한은 운영체제(OS) 뿐만아니라 OS레벨에서 운영되는 모든 어플리케이션의 설정을 변경하거나 ON/OFF할 수 있는 막강한 권한이다. 농협사태를 보면 ROOT권한에서 모든 파일삭제(rm)명령이 내려진 것이다. 모든 파일삭제 명령어는 관리자의 부주의나 실수 또는 조직에 불만이나 앙금이 있는 관리자의 악의적인 데이터 파괴 공격과 해킹에 의한 ROOT권한 탈취 등 다양한 변수에 의해서 언제든지 전산시스템을 마비시킬 수 있는 명령어이다. 이러한 절대 권한을 아웃소싱 업체에 부여한 것 뿐만아니라, 인력 및 접근 가능한 단말기에 대한 정보보호체계의 부실로 인해 초유의 금융전산망 마비사태가 발생하였다[5].

2.2 전산운영시스템의 접근 시 문제점

2.2.1 접근 권한

해당 사용자는 운영시스템에 접근할 수 있는 권한이 있는가하는 부분에 대해서는 기관들이 서로 다른 접근방법을 가지고 있을 수 있다. 대부분의 기관들은 인증요청 관리를 위해 새로운 권한 발행시스템이나 변경시스템을 사용할 것이다. 발행시스템의 경우, 권한이 부여되지 않은 사용자의 접근을 과연 확실히 차단하는 것인지에 대해서는 생각해 볼 문제이다.

접근제어 솔루션은 사용자 개인을 시스템에 인증시키고자 할 때 사용된다. 여기에서 문제는 유효한 사용자는 과연 바로 권한이 있는 사용자인가 하는 부분으로, 유효한 사용자의 적합성의 여부가 인증되었는지 확실하지 않다는 것이다[6][7].

2.2.2 변경 권한

해당 사용자는 운영시스템을 변경할 권한이 있는가의 경우, 접근 관리에 직접적으로 해당되는 내용이다. 대상 타깃시스템에서 보안 관리는 접근권한 수준에 따라 변경을 허가 하거나 거부할 수 있는 영역이다. Unix를 예로 들었을 때, 시스템 관리자는 기본적인 문제해결을 위해 userid를 사용하지만 작업에 따라 많은 사항들의 변경이 요구되는 경우는 'root' 권한의 접근을 필요로 하게 된다.

또한 개인계정 부여 등 개인사용자의 접근성에 대한 균형도 조정해야 한다. 일반적으로 개발자 userid 계정을 사용하면 사용자 관리 면에서는 매우 편리하지만, 타깃 대상시스템 상에서 공용으로 이 계정을 사용하는 각각의 개인 별 내용은 관리할 수 없게 된다. 반면에, 각 개발자, 데이터베이스 관리자, 시스템 관리자 별로 고유한 userid를 부여하는 경우에는 상당한 관리 및 유지보수 작업이 필요하게 된다.

2.2.3 변경 시 작업의 정확성 검증

해당 사용자는 인증된 변경작업만 진행하였는가? 변경작업은 정확하게 이루어졌는가 하는 내용은 바로 신문기사의 머리제목으로 자주 등장하는 문제이면서도 가장 감지하기 어렵고, 해결하기 어려운 부분이다. 정상적으로 권한이 부여된 유효한 사용자는 과연 필요한 변경작업만을 수행하였는가, 변경작업이 변경관리시스템을 통해 이루어졌다면, 대부분의 자동화된 프로세스는 변경 전, 후의 비교를 위한 원본소스 제공과 모든 이동에 대한 보고가 이루어지며, 시스템 변경 전, 후의 상태에 대한 매우 자세한 내용을 제공한다. 그러나 개발자가 문제가 발생한 어플리케이션의 운영시스템에 접근하는 경우, 실질적인 문제는 감사를 위한 추적이 아니라, 가용성 즉, 어플리케이션의 정상적인 운영이다. 접근개발자 개인에게 악의가 없었다 하더라도, 대부분의 개발자들은 그들이 문제해결을 위해 무엇을 했는지 정확하게 설명하도록 가중한 압력을 받는 것이 현실이다. 이러한 이슈가 결국, 페니 메이(Fannie Mae-연방저당공사 증권) 사건의 발단으로 이어져, 내부직원이 설치한 악성코드로 4,000대가 넘는 서버의 모든 데이터가 파괴되는 일이 벌어지기도 하였다[8].

Ⅲ. 시스템 접근통제 관리 방안

3.1. 체계적인 시스템 접근통제 방안

계정 및 권한관리의 문제점인 퇴사자 계정/공용 계정 존재, 패스워드 관리, 사용자 현황 파악, 계정정책 일관성 부재, 책임발생 시 추적, 시스템 접근원칙 등을 표 1과 같은 정책을 통해 보안을 강화한다.

표 1. 계정 및 권한관리 방법

구분	조치 방법
계정관리	– 직원의 퇴사 시 바로 계정을 Blocking 하도록 조치 – 임시계정의 경우 일정기간 뒤에 자동 Block하도록 함
1인 1계정	– 공용계정 사용을 없애고, 1인1계정을 사용하도록 함 – Super계정의 경우 APPS에서 사용되지 않도록 함
접근강화	– Super사용자의 직접로그인 통제 – Role 기반의 시스템 계정 발급 체계화
감사	– 사용자의 계정 발급 및 변경 이력 감사 – 사용자의 시스템 접근 이력 추적
암호정책 강화	– 주기적으로 암호변경을 하도록 정책 적용 – Selfservice를 통한 암호관리강화

Ⅳ. 시스템 접근통제를 위한 패스워드 관리 방안 연구

통합시스템의 접근을 통제하기 위한 패스워드 관리 방안은 개발자가 운영시스템에 접근 시 접근권한, 변경권한, 변경작업 시 신뢰된 접근의 안전성을 확보 및 정확성 검증을 반드시 하여야 한다.

4.1 접근 권한 관리 방안

시스템 접근 시 사용자가 운영시스템에 접근해야 하는지 판단한다. 접근이 필요한 경우 사용자는 특정 타깃, 대상시스템으로 접근 요청을 보낸다. 이 과정에서 다른 사용자의 승인을 받거나 티켓팅 시스템에 실시간 인증요청을 보낸다. 이 방법은 생산 시스템의 자동 로그인 등 계정의 크리덴셜 전반을 관리함으로써 사용자가 접근권한관리시스템을 거치지 않고 바로 운영 시스템에 접근할 수 없도록 차단한다. 사용자는 패스워드를 알 수 없기 때문에 크리덴셜 또한 절대 노출되지 않는다.

접근권한관리시스템에서 사용자란 유효한 권한으로 승인된 사람을 의미한다. 그림과 같이 일단 승인된 사용자에 대해서는 접근을 요청한 운영시스템에 프록시 연결을 설정한다.

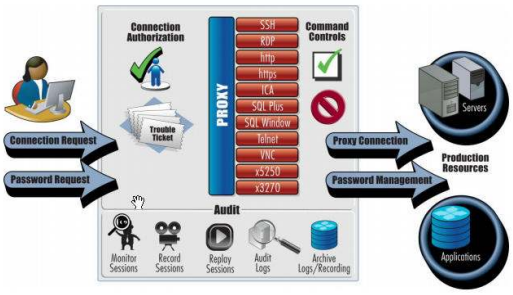

그림 1. 접근권한관리시스템 구성도

또한 접근권한관리시스템은 기존의 AD, LDAP 혹은 CMDB 환경을 쉽게 통합하여 디렉토리/CMDB 수준에서 프로비져닝된 사용자나 시스템, 계정이 자동으로 접근권한관리시스템에 동기화되도록 한다. 특히 백엔드 티켓팅 시스템과 완벽 통합을 지원해 티켓팅 시스템의 DB 쿼리가 접근권한에 활용 될 수 있도록 한다.

4.2 변경 권한 관리 방안

접근권한관리시스템은 공유계정 패스워드 관리를 제공해 루트나 기타 접근에 사용되는 계정의 관리를 돕는다. 접근권한관리시스템은 개별 사용자의 접근성을 제공하기 때문에 일반 userid가 타깃 시스템에 사용될 수 있도록 한다. 따라서 기업은 개별 사용자의 접근성을 희생시키지 않고도 운영 시스템의 특정 계정에 관리 과부하가 일어나는 것을 방지할 수 있다.

또한 접근권한관리시스템은 권한 명령 관리를 지원해 개인 사용자들도 명령 및 환경에 대한 실행 권한은 배제된 채 운영환경에 접근할 수 있다.

4.3 변경 작업 시 정확성 검증 방안

접근권한관리시스템은 무슨 작업을 했는가 라는 질문에 대한 답을 세션 모니터링과 기록 기능을 통해 제시한다. 모든 키보드 입력과 마우스 동작, 어플리케이션 접근은 모니터링 되어 기록, 저장되며, 이 자료는 호스트 기반의 에이전트 소프트웨어 설치 없이 이후 감사 및 포렌식에 사용된다. 세션 기록은 동작이 있는 경우에만 이루어지며(비 동작 시 기록하지 않음), 보안과 저장공간의 효율성을 위해 압축/암호화 된다. 또한 세션 로그관리를 통해 재생한다.

실시간 모니터링이 필요한 요구사항을 만족시키기 위해 접근권한관리시스템 세션 모니터링은

감사 담당자와 리뷰, 적합한 권한을 갖는 관리자가 액티브 세션을 확인할 수 있도록 한다.

커멘드. 즉, 명령어 수준의 통제와 감사는 그들이 무엇을 했는가 라는 수준에서 인증된 권한을 가지고 무엇이 가능했는가에 대한 관리로 확장시킨다.

V. 결 론

접근권한관리시스템은 개발자들이 각 개인별로 관리되는 계정을 사용하여 반드시 필요한 경우에만 운영시스템에 접근할 수 있도록 하며, 이런 접근에 대해서는 철저한 감사 및 통제가 이루어진다. 타깃 대상계정의 관리를 통해 우회접근 시도를 방지하는 내장된 매카니즘은 누가 운영시스템에 접근하였고 누가 권한을 획득 했는지, 그리고 그러한 접근을 통해 무슨 작업이 진행되었는지 명확하게 파악할 수 있다. 또한 접근이 승인된 사용자가 무엇을 할 수 있는지 보다 인증된 사용자가 할 수 있는 작업에 대한 세밀한 관리와 통제가 가능함으로써 개발자들의 운영시스템 접근과 관련된 보안 및 컴플라이언스 이슈에 해답을 제시한다.

향후 연구로는 접근권한통제, 실시간모니터링, 유해침입 자동감지, 로그관리 및 감사 기능을 통합으로 관리하는 통합보안운영관리시스템을 연구하여 수많은 보안사고를 사전에 차단하고, 만일 발생한 위협에 대해서 능동적인 즉각 대처가 가능하도록 하겠다.

참고문헌

[1] 변순정, "개인정보 유, 노출 등의 통지 관련 국내외 법제 현황," 한국정보보호학회지, 제 18권, 제 6호, 35-42쪽, 2008년 12월.

[2] 행정안전부, "개인정보의 안전성 확보조치 기준 및 해설서", 2011년 9월.

[3] Jong-Il 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.

[4] 남기효, "개인정보보호기술의 최신 동향과 향후 전망," 한국정보보호학회지, 제 18권, 제 6호, 11-19쪽, 2008년 12월.

[5] Jong-Il Baek, "A Study of Disaster Preparedness Systems Operations Analysis and Financial Security Mesures of Large Banking Network." ICHIT 2011, CCIS 206, pp. 167-173. September 2011.

[6] 이강석, "데이터베이스 사용자 사전 통제 및 사후 추적을 통한 데이터베이스 보안 연구," 한양대 공학대학원, 2007년 2월.

[7] 문형진, "역할기반 접근제어시스템에 적용가능한 민감한 개인정보 보호모델," 한국컴퓨터정보학회논문지, 제 13권, 제 5호, 103-110쪽, 2008년 9월.

[8] 백종일, "DB 보안의 문제점 개선을 위한 보안등급별 Masking 연구," 한국컴퓨터정보학회논문지, 제 14권, 제 4호, 101-109쪽, 2009년 4월.

[9] 남원희, 박대우, "입법기관의 보안강화를 위한 Cloud 네트워크 분석 및 보안 시스템 연구," 한국해양정보통신학회논문지, Vol.15, No.6, pp.1320-1326, 2011년 6월.