근태관리 중심으로 보안성을 향상시킨 2-Factor 인증 계정관리시스템

최경호* · 김종민** · 이동휘***

요 약

오늘날은 다수의 정보자산 내 중요 데이터를 다수의 사용자가 필요에 의해, 필요한 만큼 접근하여 열람하고 있는 정보화 사회이다. 이러한 복잡함 속에서 중요 정보 자산에 대해 허가된 사용자의 접근을 확인하고, 사용 이력을 관리하기 위해 계정 관리 관련 기술이 적용되고 있다. 그러나 계정을 이용해 중요/민감 정보를 열람할 수 있다는 점은 이것이 탈취 당했을 때 공격자에게 정보 절취의 길을 열어줄 수 있게 된다는 단점이 있다. 따라서 본 논문에서는 계정 소유주의 근태에 기반하여 계정의 사용 유무를 통제할 수 있으면서도, 보안성은 높였고, 편의성 저해도 없는 안전한 계정관리시스템을 제안하였다. 제안된 시스템은 계정 소유주가 업무 목적으로만 계정을 사용할 수 있도록 허가된 기간 내에 2-Factor 인증을 통해 로그인을 허용한다. 이를 통해 계정 유휴 기간 내 발생할 수도 있는 정보 유출을 사전에 차단할 수 있다.

Identify Management System with improved security based working time supervising

Kyong-Ho Choi* · Jongmin Kim** · DongHwi Lee***

ABSTRACT

Today, it is an information society where a large number of users access and view important data in a large number of information assets as needed. In this complexity, techniques related Identify Management are being applied, in order to verify authorized user access to important information assets and manage of history. But, the ability access to sensitive information using account has the disadvantage of being able to open the way for information to the attacker when it is hijacked. Thus, in this paper, we propose a secure Identify Management System that can control the use of accounts based on the attitude of the account holder, but also enhances the security and does not hinder the convenience.

Key words : 2-Factor Authentication, Identify Management, Information Security, Prevention Data Leakage, Security Management

접수일(2017년 11월 30일), 수정일(1차: 2017년 12월 27일), 게재확정일(2017년 12월 29일)

* 싱크빌리지 주식회사 기업부설연구소장
** 경기대학교 융합보안학과
*** 동신대학교 융합정보보안학과(교신저자)

1. 서 론

오늘날은 컴퓨터 등의 정보자산을 이용한 업무처리가 너무도 당연하게 여겨지는 정보화 사회이다. 컴퓨터와 네트워크를 이용한 비즈니스가 발전하면 발전할수록, 그 규모가 커지면 커질수록 이용되는 정보자산의 수도 증가한다. 이와 더불어 해당 정보자산에 접속하여 업무처리를 하는 사용자 수도 함께 증가한다.

이러한 환경에서 정보자산 내 데이터와 같은 자원을 다수 사용자가 공유하고, 보안 등급에 따른 접근 가능 정보들을 통제하기 위해 계정관리(Identity management) 관련 기술이 적용되고 있다[1]. 계정관리는 정보 자산에 대한 사용자의 접근을 확인하고, 사용 이력을 관리할 수 있다는 장점이 있으나, 계정을 이용해 중요/민감 정보를 열람할 수 있다는 점은 이것이 탈취 당했을 때 공격자에게 정보 절취의 길을 열어줄 수 있게 된다는 단점이 있다. 특히, 2016년 버라이즌(Verison)에서 발표한 데이터유출조사보고서에 의하면 데이터 유출 사고의 63%가 계정을 활용했다고 지적한 것과 美 국가안전보장국(NAS) TAO(Tailored Access Operations) 그룹 총 책임자인 롭 조이스(Rob Joyce)가 네트워크 침투 시 계정 탈취를 주로 이용한다고 밝힌 사실은 계정 관리에 대한 보안의 중요성을 더욱 잘 인식시켜주고 있다 하겠다[2].

그러므로 계정은 적법한 사용자가 원할 때는 언제든지 사용 가능하여야 하지만, 원하지 않거나 탈취 당했을 때에는 사용되지 않아야 한다. 따라서 본 논문에서는 사용자가 계정을 사용해야 하는 때를 업무 관점에서 정의하고, 이를 시스템적으로 자동화 지원하여 계정이 비활성화 되어야 하는 시기의 비인가 된 사용을 방지함으로써, 안전하게 내부 정보를 관리할 수 있는 방법을 제안하고자 한다.

이어지는 2장에서는 관련 연구로 계정을 이용한 인증 외 다른 수단들에 대해 살펴보고, 업무 목적 상 사용되는 계정의 활성화 절차에 대해 알아보고자 한다. 그리고 3장에서 본 논문에서 제안하는 계정관리 구조를 제시하고, 4장에서 시나리오를 이용해 제안된 모델의 실증 분석을 수행한다. 마지막으로는 본 연구에서의 한계와 향후 계획에 관해 논의하기로 한다.

2. 관련 연구

2.1 계정관리시스템

증가하는 정보시스템에 따라 사용자 계정 또한 나날이 증가하고 있으며, 이에 따라 업무 계정을 본인 스스로 관리하기 어렵게 되어 계정관리 관련 시스템들이 적용되게 되었다[3]. 더욱이 자동화되지 않은 계정관리 비용이 계정당 51달러에서 147달러까지 이르는 것으로 가트너그룹이 발표했던 바와 같이, 비용 상의 이점과 관리 상의 편의로 인해 정보관리 측면에서 보편화된 시스템으로 인식되며, 그 영역을 넓혀왔다.

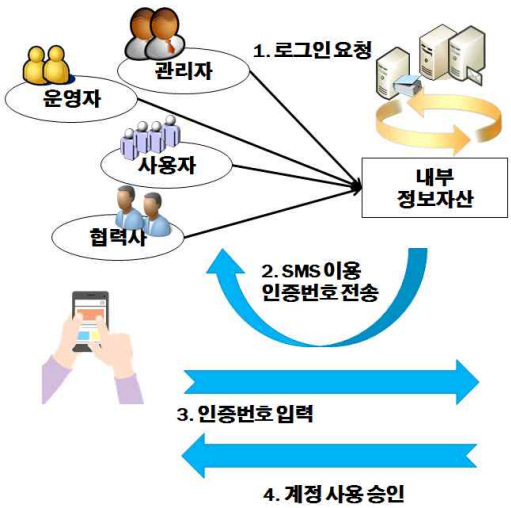
이 계정관리시스템은 ID/PW를 저장한 서버에서 단일인증(Single Sign On) 기능을 제공하며, 관련성이 있는 경우에만 해당 업무와 정보에 접근을 허용하는 역할기반(Role-based) 인증체계로 발전해왔다. 이 방식은 정보 접근자를 식별하고 사용 내역을 확인하기에는 좋으나, ID/PW의 분실 또는 절취가 발생하였을 경우, 악의적 공격자가 원 계정의 소유주와 동일한 권한을 사용할 수 있게 된다는 문제점이 있다.

2.2 2-factor identification

ID/PW를 이용한 인증은 사용자에게 수월하게 적용할 수 있으나, 이용자들이 인증정보를 비슷하게 사용하고 있는 환경에서 주기적으로 PW를 변경하고 강력하게 구성하도록 유도하는 것은 현실적으로 불가능해 보인다. 또한 개별 사용자에게 PW 관리에 대한 모든 책임을 부과할 수 없기 때문에 보안성 강화와 편의성의 최대화에 기반을 두고, 양방향 이중 인증(two factor authentication) 방식을 적용할 필요성이 제기되었다[4]. 그리고 이중 인증은 보안 수준의 향상을 위한 효과적인 방법으로 응용되고 있다[5].

이중 인증에서는 SMS를 이용한 방법이 많이 활용되고 있다[6]. 이것은 사용자가 미리 등록해둔 전화번호로 메시지를 보내 사용자가 그에 맞는 값을 입력하도록 함으로써, 사용자가 소유하고 있는 것을 토대로 한 번 더 인증을 수행하는 것이다. 그러나 추가 인증 단계에서 소요되는 시간과, 매번 추가 인증을 실시해야 하는 번거로움이 있다. 또, 물리적으로 스마트폰 등 이중 인증에 사용되는 장치의 도난, 이중 인증 관련 메

시지의 절취 등에 취약한 문제점도 있다.



(그림1) SMS를 이용한 2-Factor 계정관리의 예

이에 대해 3-Factor 인증이 제안되기도 하는데[7], 이는 다중 방어 측면에서 좋기는 하나, 인증 단계 증가로 인한 시간 소요와 사용자 불편도 함께 증가한다는 단점도 있다.

2.3 근태관리를 이용한 업무 관련 사용계정 확인

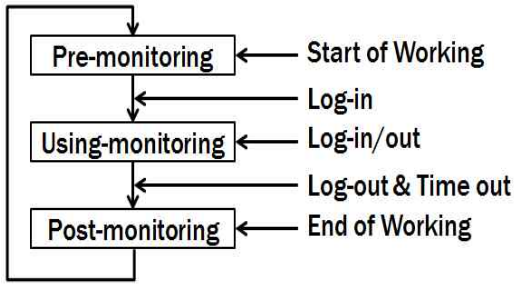
인증 단계의 증가가 보안성을 강화시키기는 하나, 사용자에게는 불편함을 초래하여 규정을 어길 유인을 가져온다는 사실 하에, 사용자가 업무를 수행하기 위해 조직 또는 기업 내부에서 진행하는 인증을 추가적으로 계정관리에 적용한다면, 별도의 사용자 행위가 없더라도 계정에 대한 2-factor 인증이 가능하다. 즉, 출입 허가 시 네트워크접근통제도 함께 수행하는 것처럼[8], 하나의 인증 정보를 다른 시스템에서 활용하는 것은 사용자에게 편리함을 줄 수 있으며, 이중 인증을 수행할 수도 있다. 이때, 2-factor 인증은 가진 것, 아는 것 그리고 자신을 증명하는 특징인 3가지 요소로 이루어져야 하며[9], 각기 다른 요소로 2가지가 적용되어야 한다. 그리고 기반으로 사용하는 인증 정보는 생체 정보와 같이 강력한 것으로 사용하는 것이 더욱 보안성을 향상시킬 수 있게 될 것이다.

이러한 맥락에서 사용자가 업무를 추진하기 위해 계정을 사용하기 전 작동하는 시스템들을 살펴보면, 대표적으로 출입통제와 근태관리의 예를 들 수 있다. 출입통제시스템은 사용자가 업무 처리를 위해 조직 또는 기업 내부로 진입하는 것을 확인할 수 있게 해주고, 근태관리는 계정 소유주의 업무 추진 현황을 알 수 있게 해준다. 따라서 출입통제와 근태관리의 정보로 계정 소유주의 계정 사용 필요성을 미리 파악해 둔다면, 이를 이용해 계정의 업무 관련으로 인한 사용 예정 유무를 판단할 수 있으며, 계정 소유주가 가진 것 또는 소유주의 특징적인 것으로 인해 2-Factor 인증 시행이 가능하다.

3. 제안하는 2-Factor 인증 기반의 계정관리모델

3.1 제안시스템 설계

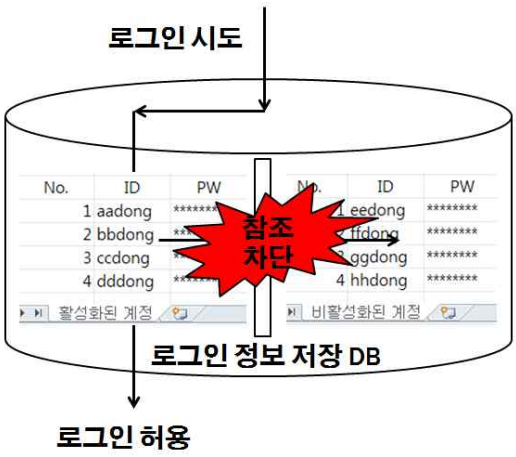
본 연구에서는 제안하는 2-Factor 인증 기반의 계정관리모델은 다음 (그림2)에서 볼 수 있는 바와 같이 계정이 사용 예약되어 언제든지 활성화가 가능한 상태인 Pre-monitoring, 계정이 사용 중인 Using-monitoring 그리고 계정의 사용이 끝나 추후에 사용될 것을 대기하는 Post-monitoring으로 크게 3계층으로 구분되며, 각각의 국면 별로 계정의 활성화와 사용이 다르게 이루어진다.



(그림2) 제안시스템의 3계층 구조

여기서 활성화된 계정이란 사용 예약이 된 계정 및 사용 중인 계정을 의미하는 것으로, 업무 추진 상 Log-in과 Log-out으로의 상태 변화가 허용된 것을 의미한다. 만약, 계정 소유주가 업무 추진 예정이 없거나,

업무가 종료되었다면 해당 계정은 비활성화 되어 Log-in 시도에 대한 응답을 하지 않는다. 이와 같은 기능 수행을 위해 계정의 로그인 정보를 담은 데이터베이스를 분할하여 별도의 테이블로 계정들을 관리하게 된다.

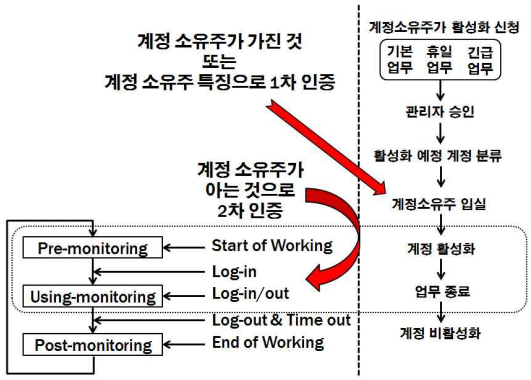


(그림3) 로그인 정보의 분리된 관리

계정을 활성화하는 방법은 계정의 소유주가 업무 목적 상 계정을 사용한다고 보고하는 근태관리 상의 시간을 기준으로 계정 소유주가 조직 또는 기업 내부에 출입하였을 때 진행된다. 즉, 계정 소유주가 계정을 사용할 계획을 가지고 계정을 사용할 장소에 도달하였을 때에만 계정이 활성화되어 Log-in/out이 가능하게 되는 것이다. 그리고 사용 중 또는 종료 후 사용 예정 위치를 벗어나게 되면 자동적으로 계정은 비활성화 상태가 된다. 이때, 출입관리시스템은 사용자가 가진 RFID, 또는 사용자를 의미하는 지문, 얼굴인식 등으로 동작하여 2-Factor 인증을 만족하게 된다.

3.2 제안시스템 동작 절차

근태관리에 기반하여 계정의 활동성 유무가 결정되는 본 제안시스템에서는 계정 소유주의 기본적인 업무 수행시간 이외에도 야근 또는 휴일 근무 등에도 계정 활성화를 수행할 수 있다. 이는 계획된 업무 외 긴급을 요하는 업무를 처리하는 현실의 상황을 시스템적으로 지원하고 있는 형태이다. 그리고 오늘날의 스마트워킹 현실을 반영하기 위해 원격에서의 계정 사용 시, 계정 소유주가 가진 기기를 토대로 인증을 수행하여 2-Factor 인증을 유지할 수 있다.



(그림4) 제안시스템 동작 절차

상기 (그림4)에 표현된 바와 같이, 본 논문에서 제안하는 시스템의 동작절차는 계정소유주가 자신의 업무 주기를 토대로 계정 사용 예정 시간을 입력하는 것으로부터 시작된다. 이 사항에 대해 관리자가 승인을 하면 계정소유주가 업무를 위해 조직 내 들어왔을 때, 해당 계정이 로그인 가능한 상태가 되는 것이다. 만약 이때, 계정소유주가 업무 목적이 아닌 내방이라면 계정이 활성화되지 않아 사용하지 못하는 상태가 되고, 이는 계정소유주가 외부에 있을 때도 자연스럽게 계정이 활성화되지 않은 상태에 머물러 있다는 것을 의미한다. 따라서 계정소유주가 업무 목적 상 내부 네트워크를 사용하는 시간대가 아니라면, 해당 계정이 활성화되지 않아 계정 탈취가 발생하더라도 공격자가 해당 계정을 사용할 수 없는 상태가 되는 것이라 불법적인 자료 절취가 발생할 가능성을 한층 낮출 수 있는 방법이 된다.

그리고 계정소유주의 업무가 종료되면, 해당 계정 역시 로그인이 불가능한 비활성화 상태로 되돌아가며, 계정소유주의 업무 시간이 다시 도래하여야만 로그인 가능한 상태가 된다.

3.3 제안 모델 평가

3.3.1 기능 평가

본 논문에서 제안한 시스템은 계정관리시스템 기반

위에서 계정 소유주가 소지하고 있는 것 또는 계정 소유주를 식별할 수 있는 정보로 2-Factor 인증을 수행하기 때문에 기존 계정관리시스템의 기능들을 모두 수행하면서도, 사용이 예정되지 않은 계정들에 대한 잠금장치를 제공하는 보안 기능을 추가적으로 제공한다.

이것은 권한 없는 사용자에 대한 정보 접근 및 열람을 제한하는 것과는 차별화된 기능으로, 계정이 사용 불가능하도록 비활성화 되기 때문에 특정 계정의 절취로 인한 악의적 사용자의 접근을 차단할 수 있다.

3.3.2 보안성 평가

본 논문에서 제안한 시스템을 사용했을 때의 가장 큰 장점은 업무 목적으로의 사용이 확인되지 않은 계정은 잠금 상태가 되어 내외부에서 이를 이용한 정보자산에 대한 접근이 허용되지 않는다는 것에 있다. 이는 계정 소유주의 비의도된 계정의 분실, 도난 등으로부터 조직 또는 기업의 중요 정보자산을 보호할 수 있는 수단을 제공하며, 계정 소유주들의 실제 계정 사용 현황을 실시간으로 파악할 수 있어 내부적인 보안관리도 강화시킬 수 있는 방안이 된다. 예로, 업무 목적 내방이 아닐 경우 불필요하게 계정이 사용될 수 있는 가능성을 사전에 차단할 수 있고, 등록된 업무 추진 시간 내 미사용 계정을 식별하여 사용자의 안전한 계정 관리 실행 여부를 관리, 감독하며 보안 교육에 반영시킬 수도 있다.

그리고 계정 소유주가 계정을 사용하고 있는 중에는 이중 로그인을 방지하여, 계정 탈취자의 악의적 접근을 차단할 수 있다. 단 시간 내에 서로 다른 지역에서 로그인되는 것을 탐지한다거나, 불확실한 지역에서의 로그인 시도, 로그인 된 상태에서의 추가적인 로그인 시도 등의 위협들을 파악하여 이에 대한 조치를 취할 수 있게 된다.

그러므로 본 연구에서 제안한 시스템을 사용하게 되면, 계정의 유휴시간과 사용시간 모두 로그인 정보 유출로부터 안전할 수 있으며, 계정 소유주의 추가적인 인증 절차 수행이 없어 편리함도 제공할 수 있는 장점이 있다.

마지막으로 내부자의 업무 목적 외 내부 출입을 확인할 수 있어, 계획된 업무 수행 외의 비정상 행위들을 파악할 수 있는 장점을 들 수 있다.

4. 결 론

본 논문에서는 계정 소유주의 근태에 기반하여 계정의 사용 유무를 통제할 수 있으면서도, 보안성은 높였고, 편의성 저해도 없는 안전한 계정관리시스템을 제안하였다. 본 연구에서 출입통제보다 근태관리에 주안점을 둔 이유는 보고 또는 지정된 업무 수행 외의 정보 자산에 대한 접근을 차단시켜 내부 정보 유출을 방지하기 위함이었다. 이는 업무 목적 외 내방도 가능하고, 정보 자산의 사용이 없는 업무 처리 기간에는 계정을 비활성화 시켜 악의적 공격자에 의한 로그인 시도를 원천 차단할 수 있기 때문에 선택되었다. 그러나 사용자가 업무 수행을 위해 사용하는 다른 정보 또는 보안시스템에서의 인증 절차가 본 논문에서 제안한 것보다 더 강력한 보안을 제공하거나 편리하다면 개선을 위해 적용 가능하다 하겠다.

참 고 문 헌

[1] Jorge W., C. M. Westphall and C. B. Westphall, "Cloud identity management: A survey on privacy strategies", Computer Networks, Vol. 122, 20, pages 29-42, July 2017.

[2] Palo Alto Networks, unit 42, Credential-based Attacks.

[3] 박병언, 양재수, 조성제, “행정업무 능률향상을 위한 통합 계정 및 접근 관리 방안”, 정보보호학회논문지, 25(1), pages 165-172, 한국정보보호학회, 2015. 2.

[4] 지선수, “SMS를 이용하는 개선된 이중 인증 기법”, 한국산업정보학회논문지, 17(6), pages 25-30, 한국산업정보학회, 2012. 12.

[5] 이극, 지재원, 천현우, 이규원, “하이브리드 클라우드 컴퓨팅 환경에 적합한 인증시스템 설계”, 정보·보안 논문지, 제11권, 제6호, pages 31-36, 한국융합보안학회, 2011. 12.

[6] Hossein S., T. Nguyen, P. Gupta, M. Jakobsson and N. Memon, "Mind your SMSes: Mitigating social engineering in second factor authentication", Computers & Security, Vol. 65, pages 14-28, Mar. 2017.

[7] 신승수, 한군희, “OTP를 이용한 HMAC 기

반의 3-Factor 인증", 한국산학기술학회 논문지, 10(12), pages 3708-3714, 한국산학기술학회, 2009. 12.
[8] 최경호, 김종민, 이대성, "RFID 출입통제시스템과 연동한 네트워크 이중 접근통제 시스템", 정보·보안 논문지, 제12권, 제3호, pages 53-58, 한국융합보안학회, 2012. 6.
[9] 서세현, 최창열, 이구연, 최황규, "QR 코드를 이용한 모바일 이중 전송 OTP 시스템", 한국통신학회논문지, 38(5), pages 377-384, 한국통신학회, 2013. 5.

〔저 자 소 개〕

최 경 호 (Kyong-Ho Choi)

2002년 경기대학교 경제학사
2005년 경기대학교 경제학석사
2008년 경기대학교 정보보호학박사
2017년 싱크빌리지 주식회사
기업부설연구소장
email : cyberckh@gmail.com

김 종 민 (Jongmin Kim)
2010년 체육학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과
초빙교수

email : dyuo1004@gmail.com

이 동 휘(DongHwi Lee)
2007년 경기대학교 정보보호박사
2011년~2012년 University of Colorado Denver, Dept. of Computer Science and Engineering
현 재 동신대학교
융합정보보안학과 교수

email : dhclub@dsu.ac.kr