본인 이력 기반 사용자 인증 방법

경호연*, 박지수**, 손진곤*
*한국방송통신대학교 대학원 정보과학과
**고려대학교 대학원 컴퓨터교육과
ganadara135@gmail.com

A User Authentication Technique Based on Self Recording History

Ho Yun Kyung*, JiSu Park**, Jin Gon Shon*
*Dept. of Computer Science, Graduate School, Korea National Open University
**Dept. of Computer Science Education, Korea University

요 약

온라인 서비스가 증가하고 있으며, 그에 따른 개인의 서비스 계정도 늘어나고 있다. 하지만 지속적으로 늘어나는 서비스 계정의 의해, 관리의 어려움과 노출 위험성이 커지고 있다. 해결책으로 보안도 유지하면서 다양한 온라인 서비스의 종류에 구애 없이 하나의 통합된 사이트를 통해서 계정정보를 관리하면 편리할 것이다. 그래서 ID/PW 방식의 사용자 인증에 감사 가능을 결합한 본인 이력 기반 사용자 인증 방법을 제안한다. 본인이 생성한 비밀번호 이력 정보에 다양한 옵션을 설정할 수 있도록 하여 사용자 인증에 사용하고, 검증 과정에 본인이 직접 참여하는 메커니즘을 결합하여 본인 이력 기반 사용자 인증 방법이 완성된다. 제안 방식을 현재 인테넷뱅킹에서 사용 중인 인증 방식들과 보안성을 비교 검증하였다.

1. 서론

일상 업무의 상당부분이 온라인으로 처리됨에 따라 개인이 가입해야하는 서비스도 증가하고 있다. 서비스 가입 시 본인 인증을 위해 ID/PW를 생성하여 사용한다. 그러나 서비스의 증가에 따라 ID/PW도 증가하게 되어 개인 계정의 노출 및 관리의 어려움도 증가한다. 이런 문제점을 해결하고자 SSO(Single Sign On)같은 통합인증기술이 도입되었으나 내부망(인트라넷)에서만 작동하고, 비연결형(HTTP) 방식의 경우, 쿠키 등을 통한 정보 유출의 취약성이 있다. 또한 ID/PW 인증체계 이외에 PKI, 생체정보 등을 활용하여 통합인증에 적용할 수 있으나, 생체정보 같은 토큰 정보 노출 시에는 재사용의 위험성이 있다. 해킹의 위협에 대응하기 위한 암호 기술은 시간이 지남에 따라 지속적으로 암호의 복잡도를 높여야 하는 어려움이 있다.

PKI, 생체정보 등과 같은 개별 보안기술의 약점을 보안하고자, 2가지 이상의 개별 보안기술을 결합하는 2-factor 인증 방식[6]도 현재 주요 사용자 인증 방식으로 사용되고 있으나, 비용의 증가하고 사용이 복잡하다.

사용자 인증 체계는 다양한 보안 기술들이 각 요소마다 결합되어 전체 체계가 구성되어 운영된다. 그러므로 시스템이 복잡해질수록 시스템 구성 및 보안이 어렵다. 보안 요소 중 가장 취약한 부분이 사용자의 고유 데이터(비밀번호 등)의 무결성 유지이다. 무결성이란 본인 이외의 다른 사용자의 데이터 조작을 막는 것이다. 고유 데이터는 사용자 본인이 유출할 수도 있지만, 시스템 내부 관계자가 유출하는 경우엔 사건이 발생되고 충분히 위용 된 후에 도용 여부가 확인되는 경우가 많다. 이런 고유 데이터의 내외부의 유출에 대응하기 위해 사용자가 직접 고유 데이터의 사용이력을 점검할 수 있어야 한다. 또한 사용자 인증 체계의 주요 문제점은 사용자 개인에 의한 키 관리(인증서, 패스워드, PIN 등)의 어려움에 있다[4],[5].

따라서 본 논문에서는 통합인증, 키 유출 위험성, 암호복잡도등의 한계를 해결하고, 쉽고 저비용적으로 고유 데이터 사용 이력을 본인이 직접 점검할 수 있는 사용자 인증 체계를 제안한다.

2. 관련연구

주요 보안 메커니즘은 암호화, 인증, 권한, 감사 등 4가지로 분류된다[1]. 암호화(encryption)는 주요 데이터를 불법적인 사용자가 사용할 수 없도록 변형하는 것이며, 인증(authentication)은 합법적인 사용자만이 이용할 수 있도록 데이터의 접근을 제어하는 기법이고, 권한(authorization)은 합법적인 사용자나 인증 받은 단위에게만 데이터의 접근을 허용하는 기법이며, 감사(auditing)는 사용자의 어떤 데이터를 어떻게 처리했는지를 기록하여 향후 검증이나 책임의 소재를 밝히는 기법이다.

인증 방식에서 사용자 인증 방법으로 패스워드, 토큰, 생체정보, 위치정보로 분류된다. 토큰은 보안카드나 보안 USB 같은 고유식별 장치를 통칭한다. 위 4가지 방식 중 보안성이 높은 방식은 신체 정보를 기반으로 한 인증방식이나 신체 특성 정보가 디지털화되어 외부로 유출되었을

때에는 영구적으로 이용 될 수 있으므로 사용 확대에 한계가 있다. 현재 대부분의 인증방식은 두 가지 이상의 인증 방식을 혼합(2 or 3 Factor)하여 사용한다. 대표적인 사용자 인증 방식들은 다음과 같다[6].

PKI 인증 방식은 클라이언트 소프트웨어를 사용 않는 방식으로 USB토큰 및 USIM 등이 있으며, 클라이언트 소프트웨어를 사용하는 방식으로는 공인인증서를 저장하여 사용하는 방식이 있다. 이와 같은 인증 방식은 인증서를 가지고 다녀야 하는 어려움이 있다.

IP-지리위치 정보식별 방식은 사용자에게 현재 할당되어 사용 중인 IP의 지리적 위치가 통상적으로 사용하는 위치인지 판단한다. 그러나 IP를 조작할 수 있다.

지문과 식별자 방식은 사용자의 정보(지문등)를 시스템의 프로파일을 저장하고 검증하는 방식이다. 파일시스템이나 전용 소프트웨어를 이용한다. 인증 방식에 있어 뛰어나나 비용이 높다.

지식기반 인증 방식은 사용자의 기억을 토대로 하여 특정한 개인 정보에 답하도록 질문을 요구하는 방식이다. 패턴이 해커에게 장시간 노출되었을 경우 위용 될 수 있다.

Out of Band 방식은 전화응답, EMail, SMS, OTP 등을 예로 들 수 있으며, 인증 과정에 같은 인증 경로를 이용 안하는 것이 핵심이다. 비용이 높고, 사용상 편의성이 떨어진다.

OTP 인증 방식은 전용단말기와 서버를 특정키와 유동적인 값(시간,주식 등)으로 동기화하여 생성되는 변수를 서로 공유하는 방식이다. 사용상 편의성이 떨어진다.

사용자 인증의 주요 문제는 MITM(Man In The Middle)인 중간자 공격이며, 이에 대응할 수 있는 인증 방법은 토큰 방식의 PKI와 Out-Of-Band 방법의 조합이다[6].

본 논문에서는 인증과 감사의 기능을 결합한 ID/PW방식으로, 사용자 편의성 및 보안성이 높은 사용자 인증 방식을 제안 한다.

3. 본인 이력 기반 사용자 인증 방법

3.1 시스템 구성

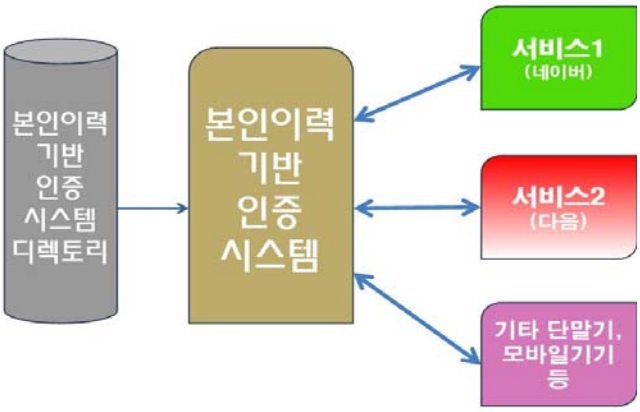
본인 이력 기반 사용자 인증이란 인증 과정에 개인 사용자가 직접 참여하여 자신의 이력 정보를 기반으로 하여 보안 검증을 하는 인증 기법이다. 참여자별로 구분하여 본인 이력 기반 인증시스템 사용 방법은 다음과 같다.

개인 사용자는 자신이 필요할 때 인증시스템에 접근하여 서비스 받길 원하는 서비스의 비밀번호를 변경한다. 그런 다음 해당 서비스 사이트에 접속하여 인증시스템에서 변경한 비밀번호로 로그인한다.

서비스 제공기관은 제안 시스템을 사용하기 위해서 비밀번호에 대한 인증을 본인이력기반인증시스템을 통해서 받는다고 등록해 놓기만 하면 된다.

본인이력기반 인증시스템에서는 비밀번호 인증 환경만을 제공한다. 그 외 개인 사용자가 자신의 이력 정보에 대해서 조사 문의가 들어왔을 때 역추적 조사 결과를 제공한다.

사용자 인증 방법의 전체적인 사용 흐름은 (그림 1)의 시스템 구성도와 같다. 기존 사용자 인증 방식은 개별사이트에서 ID/PW 방식을 이용하여 수행했다면, 제안 방식은 비밀번호 인증만을 따로 관리하여 통합적으로 (그림 1)과 같이 본인이력기반 인증시스템에서 인증을 한다. 이와 같은 방식은 아이핀(I-Pin)[2]과 비슷하게 비밀번호 인증을 전담하는 체계이다



(그림 1) 시스템구성도

3.2 작동방식

본인 이력 기반 사용자 인증은 등록단계와 활용단계로 나눠진다. (그림 2)는 본 사용자인증 체계에서 사용자 인증의 등록단계로서 참여자 간의 시간 흐름에 따른 메시지 흐름을 나타낸다. 개인 사용자(A)는 본인이력기반 인증시스템에서 서비스 제공 받을 사이트의 ID, 비밀번호 등을 등록하고, 서비스 제공 사이트에서 회원가입을 수행한다.

A2에서 인증시스템 주소입력은 본인이력기반 인증시스템의 전용 주소이다. 본인이력기반 인증시스템은 한 개가 아니라 여러 개가 있을 수 있으며, 서비스제공기관에서 개인 사용자가 입력한 전용 주소를 임의로 변경할 수 없다.

(그림 2) 본인이력기반 사용자인증 프로세스(등록단계)

(그림 3)은 활용 단계로서 임시 비밀번호를 생성하여 개별사이트의 서비스를 사용하는 과정과 본인이력기반 인증시스템에 접속하여 이력정보를 확인하여 위용여부를 검증한다.

(그림 3) 본인이력기반 사용자인증 프로세스(활용단계)

(그림 4)은 인증시스템의 테이블 구조도이다. 사용 비밀번호는 다양한 옵션(사용횟수, 사용기간, 기록활성화간격 등)을 설정할 수 있도록 되어있다. 테이블에서는 가장 최근에 기록된 정보(그림 4에서 4번째 행)만이 활성화되어 작동한다. 이전 정보의 기록은 사용자가 자신이 행한 행위인지 검증자료로써 확인한다. 기록활성화간격 옵션은 임시 비밀번호를 생성한 시간으로부터 임시 비밀번호가 비활성화되는 시간으로, 해당시간이 경과한 이후에 정상적으로 비밀번호로서 작동하게 된다. 본 옵션은 다른 사용자가 본인이력기반 인증시스템을 위용하려고 할 때 검증할 수 있는 기회를 부여한다.

(그림 4) 본인이력기반 인증체계 테이블구조도

3.3 보안 방법

제안 방식은 인증과 감사가 결합되어 있는 방식이다. 인증은 ID/PW를 기반으로 수행하며, 감사는 PW의 이력정보를 확인할 수 있도록 함으로써 위용여부를 검증 한다. 또한 임시 비밀번호에 다양한 옵션을 설정하여 보안 레벨을 높일 수 있다.

기존의 사용자 인증 방식들은 보안성을 강화할 경우 사용자의 편의성이 떨어지거나, 비용이 높아진다[6]. 그러나 제안 방식은 다음과 같은 세 가지 방식으로 보안성을 유지하면서 비용과 편의성을 제공한다. 첫째는 인증시스템에 기록한 비밀번호는 가장 최근의 내용만 활성화되어 인증정보로 작동하므로 기록을 남겨야만 사용할 수 있다. 그러므로 사용자는 본인 이력 정보를 확인하는 것으로 침입 및 위용 여부를 쉽게 추정할 수 있다. 둘째는 본 인증시스템에 내부 자료가 남의 의해 인출되거나, 노출된다고 해도 다른 곳에서 사용할 수 없는 무의미한 인증정보이다. 인증정보를 사용하기 위해서는 서비스제공기관에서 비밀번호를 인증받기 위해서 접근해야 하는 주소가 고정되어 있고, 또한 본인이력기반 인증시스템 내에서만 인출된 해당 인증정보가 비밀번호로서 작동한다. 셋째는 비밀번호는 사용자의 의해 언제든 변경될 수 있다.

<표 1> 주요 침해경로별 보안방법

침해 경로	원인	대응방법
인증 시스템 (서버)	1. 관리자에 의한 위용 2. 외부침입(해킹)에 의한 위용 3. 사용자 계정 노출에 의한 위용	세 가지 경우의 위용 확인을 위해선 (그림 4)처럼 기록을 남기므로 추적할 수 있다 예) 임시 비밀번호 기록 후 기록활성화간격 옵션부여로 기간 내 위용기록 검증가능성 부여한다.
통신 채널	1. 인증시스템과 개별사이트 사이 2. 인증시스템과 개인사용자 사이	1. 개별사이트별로 비밀시리얼키로 통신채널 설정한다(SSL). 또한 통신채널에 흐르는 데이터는 언제든 재생성이 되는 임시 비밀번호이다. 2. SSL 등의 암호화 통신을 한다. 통신채널에서 빼간 데이터는 외부에서 사용불능(무의미)하고, 변조 시 본인 검증과정에 나타남.
사용자 단말기	Trojan, 키로깅, 메모리해킹	인증시스템의 대응방법과 같다. 위용 되었다는 것을 확인 후 기록활성화간격 옵션 값 이내에 새로운 임시 비밀번호를 생성한다.

<표 1>의 대응방법에서 인증을 받기 위해선 본인이력기반 인증시스템에 기록(비밀번호)을 남겨야하고, 사용자는 또한 인증시스템에 기록된 내용을 확인하여 검증할 수 있는 체계를 제공한다. 사용자 인증을 위해 기록한 임시 비밀번호가 (그림 4)의 기록활성화간격처럼, 하루 또는 일주일 등, 특정기간이 지난 이후에 인증자료로서 사용될 수 있도록 설정함으로써 사용자가 검증과정에 참여할 수 있는 기회가 확대된다. 그러므로 본 인증체계는 내외부의 보안성이 확보된다.

4. 비교분석

본 연구에서는 보안성 및 편의성 측면을 강조하기 위해 국내의 인터넷 뱅킹 사용자 인증방식과 비교한다. Two-Channel 방식-[3]에서 사용한 비교 대상에 제안 방식을 추가했다. 비교 방식별 취약점을 추정하기 위해 요소별로 보관수단, 입력수단, 유출경로를 <표 2> 같이 나눴다.

제안 방식은 비밀번호를 숫자와 영문소문자의 조합으로 길이를 6자로 하였다. 보안성 비교를 위한 공격 유형으로 무차별 공격, 암호문 단독공격, 메모리 해킹(클라이언트), keylogger, MITM(Man In The Middle)을 다룬다. 또한, 해당 공격 유형들은 PKI가 탈취되었음을 가정 하였다.

<표 2> 기존 인터넷 뱅킹방식과 편리성 및 보안성 비교

인증 / 요소	기존 인증방식			제안 방식
	PKI + 보안카드	PKI + OTP	HSM + 전화인증 or OTP	
보관수단	PC, 매체	PC, 매체	PC, 매체	서버DB
입력방식	키보드	키보드	키보드 + 음성(키패드)	키보드
유출경로	PC 해킹, 도난, 분실	PC 해킹, 도난, 분실	PC 해킹, 도난, 분실	서버해킹, 내부자
보안요소	인증	인증, 임시비밀번호	인증, Out-Of-Band	감사(기록), 임시비밀번호
무차별 공격	$1/10^4$	$1/10^6$	$1/(2^{2048}\times N)$	$1/(10+26)^6$
암호문 단독공격	$1/10^4\times$(1-번호 매칭율)	$1/10^6\times$(1-시간당)	$1/(2^{2048}\times N)$	$1/(10+26)^6\times$(1-문자 매칭율)
메모리 해킹	가능	가능	불가능-전화, OTP-가능	가능 (검증기회부여), 무의미
Keylogger	가능	불가능	불가능	가능 (검증기회부여)
MITM	가능	가능	불가능-전화, OTP-가능	불가능(검증위치고정)

<표 2>의 무차별 공격 및 암호문 단독 공격에서 사용된 수식은 공격유형에 따른 공격 성공률을 나타낸다. 보안카드의 입력 값은 4자리 10진수, OTP는 6자리 10진수로 사용하였다. HSM는 인증서 생성에 필요한 값($1/2^{2048}$)과 전화인증 및 OTP등의 다른 공격 성공률(N-둘중 하나)이 더해진 값이다. 제안 방식은 10진수와 영문 소문자 26자가 6자리이며, 중간자공격(MITM)의 경우는 서비스 제공자와 인증 시스템간의 전용회선(가상사설망 포함)에 의해 안전성 확보가 가능하다. 중간자공격은 통신채널 상에서 이루어지므로 통신채널을 전용망으로 쓰면 데이터유출의 가능이 적다. 또한 매번 사용자 비밀번호가 생성에 의해 변경되므로 전용통신망 공격의 의지를 꺾을 수 있다.

인증방법에 상관없이 메모리 해킹을 통해 사용자 pc의 메모리 영역을 조작하여, 데이터 정보를 변경할 수 있다[3]. 그러나 제안 방식은 사용자 PC 메모리해킹으로 본인이력기반 인증시스템에 비밀번호를 생성하여도 임시 비밀번호가 바로 활성화되지 않는다. 기록활성화간격 옵션의 값만큼 2일 또는 1주일 뒤에 비밀번호로 사용할 수 있기 때문에 사용자가 인증시스템의 기록된 내용을 검증할 수 기회가 있다.

5. 결론

본인이력기반 인증체계는 기존의 인증체계와 다르게 개인 사용자가 중심이 되어 인증과정에 참여함으로써 사용상의 편의성 및 보안성을 높인 기술이다. 즉 제안 방식의 사용자 인증은 기존의 인증체계와 다르게 통합적으로 사용자 인증을 수행한다. 또한, 비밀번호 생성 이력을 사용자가 검증 가능하여 보안성을 확보했다. 기존 인터넷 뱅킹방식과 비교하여 편리성 및 비용면에서 강하고, 현재 주요 공격 유형인 메모리해킹 및 MITM에서도[6] 대응할 수 있다.

향후 연구에서는 실제 시스템을 구축하여 자료 유출 및 침입 등이 발생했을 시에 제안 방식이 보안성을 유지하면서 사용자의 편의성을 제공하는지 확인하고자 한다.

참고문헌 목록

[1] William Stallings, Cryptography and Network Security Principles and Practice, Fifth Edition.

[2] 이재신, 손병록, 구자현, 전자 ID지갑 시스템 기반의 i-PIN 고도화 기술 개발 및 구현, 한국정보보호진흥원, 2007. 12.

[3] 유한나, 인터넷 뱅킹 환경에서 사용자 인증 보안을 위한 Two-Channel 인증 방식, 한국통신학회논문지, 2011. 8.

[4] Sonia Chiasson, Issues in User Authentication, 2007.

[5] HP 교육자료, https://hplearn.co.kr/upload/old_hpLearn_upload/myclass/report/result/Type_D_CSJ_hit2050046340924.doc, 마지막접속날짜(20140408).

[6] 김현승, 클라우드 컴퓨팅과 개인 인증 서비스, 정보보호학회지, 2010. 4.