https://doi.org/10.5392/JKCA.2019.19.07.421

일회용 세션을 활용한 인증정보 기반의 사용자 인증 방안

User Authentication Mechanism based on Authentication Information using One-time Sessions

박영수, 이병엽
배재대학교 사이버보안학과

Yeong Su Park(unpys95@gmail.com), Byoung Yup Lee(bylee@pcu.ac.kr)

요약

현재 사용자 인증에는 지식기반(ID/PW 등)인증과 생체기반(홍채/지문/정맥 인식 등)인증, 소유기반(OTP, 보안카드 등)인증 등 다양한 종류의 기술을 사용하고 있다. 지식기반 인증인 ID/PW인증 기술은 구현 및 유지보수 비용이 적게 들며, 사용자에게 익숙한 방식이라는 장점에도 불구하고 해킹 공격에 취약하다는 단점을 가지고 있다. 다른 인증 방식들은 ID/PW인증기술에서의 취약점을 해결하였지만, 초기 구축비용과 유지보수 시 비용이 많이 발생한다는 점과 재발급 시 번거로운 문제점을 가지고 있다.

본 논문에서는 기존의 ID/PW기반 인증 기술보다 보안성과 편리성을 증진시키고, 인증에 사용되는 기기에 제약이 없는 사용자 인증을 안전하게 할 수 있는 방안을 제안한다.

■ 중심어 : | 사용자 인증 | 일회용 세션 | 인증 시스템 | 클라우드 |

Abstract

Nowadays, various type of technologies are used for user authentication, such as knowledge based(ID/PW, etc.) authentication, biometric based(Iris/fingerprint/vein recognition) authentication, ownership based(OTP, security card, etc.) authentication. ID/PW authentication technology, a knowledge based authentication, despite the advantages of low in implementation and maintenance costs and being familiar to users, there are disadvantages of vulnerable to hacking attacks, Other authentication methods solve the vulnerability in ID/PW authentication technology, but they have high initial investment cost and maintenance cost and troublesome problem of reissuance. In this paper, we proposed to improve security and convenience over existing ID/PW based authentication technology, and to secure user authentication without restriction on the devices used for authentication.

■ keyword : | User Authentication | One=time Session | Autnentication | Cloud |

I. 서 론

사용자가 개인PC와 스마트 기기(스마트폰, 스마트워치, 태블릿 등, 이하 본 논문에서는 '스마트폰' 이라고 한다.)를 이용해 정보 시스템에 접근하기 위해서는 사용자 인증을 통해 정당한 사용자인 사실을 증명해야한다. "사용자 인증" 기술에는 지식 기반(ID/PW)인증과 생체기반(홍채/지문/정맥인식)인증, 소유기반(OTP,보안카드)인증 등 다양한 종류의 인증기술들이 있다[1].

ID/PW인증 기술은 타인과 사용자가 중복되지 않은

* 이 논문은 2019학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임
접수일자 : 2019년 05월 28일
수정일자 : 2019년 06월 28일
심사완료일 : 2019년 06월 28일
교신저자 : 이병엽, e-mail : bylee@pcu.ac.kr

유일한 사용자임을 식별하기 위해 ID를 입력한 후, PW를 입력함으로써 해당 ID의 정당한 사용자인지 확인하는 것으로 이 기술의 장점은 구현 및 유지보수 비용이 적게 들며, 사용자에게 익숙한 방식이다. 이와 같이 편리성과 장점에도 불구하고 ID/Pw인증 방식은 브루트 포스, 키로깅, 스니핑 등의 공격[2][3]에 취약하며 이러한 악의적인 공격에 대응하기 위해서는 사용자가 복잡한 패스워드 조합 규칙에 따라 주기적으로 비밀번호를 변경하고 공인 인증서나 OTP, 홍채/지문 인식 같은 추가적인 인증 방식을 활용해야 한다.

공인인증서와 OTP의 경우 사용자에게 보안토큰을 발급하거나 재발급하는 과정에서 비용이 발생하는 문제와 분실 및 도난 시 사용자 인증을 하는데 있어 인증서 재등록 등 절차상 번거로움이 발생 하게 된다.

반면 홍채/지문 인식 같은 생체기반 인식은 지문, 안구 등과 같은 사용자의 고유한 특성을 이용해 PW와 같이 악의적인 공격자에게 도용되거나 복제되어 이용될 수 없다고 알려져 있으며, 변경 또는 분실의 위험성이 없다는 장점을 가지고 있어 많은 인증 시스템에서 활용되는데 해당 방식은 초기 구축 시 비용이 많이 발생하는 문제점과 고유한 특성을 사용해 복제나 도난 될 수 없다는 점과 달리 오히려 인증요소로 사용되는 부분이 공개되어있어 공격자에게 도용 또는 복제의 위험성[4]을 가지고 있다.

본 논문에서는 기존의 사용되는 ID/PW 인증 기술보다 보안성과 편의성을 증진 시키고, 사용자가 ID를 지정하면 스마트폰 전용 어플리케이션에서 1회용 세션을 기반으로 PW를 로그인 시 마다 매번 자동으로 갱신하여 PW기억 부담과 주기적 변경 부담을 없앴다. 또한 사용자의 기기나 장소에 제약이 없이 데이터에 접근할 수 있도록 도움을 주는 서비스인 클라우드[5-8]을 활용하여 생성된 인증정보를 클라우드 서버에 암호화 하여 저장해 사용자의 기기에는 인증정보가 남지 않아 스마트폰 도난 또는 분실로 인한 PW탈취의 위험 또한 방지할 수 있도록 설계 하였다. 또한 보안 정책이나 분실 등으로 인해 스마트폰을 사용하지 못하는 환경에서도 사용할 수 있도록 지정 PC전용 어플리케이션을 이용해 필요 시 즉각적으로 사용할 수 있도록 하였다. 이를 통해 ID/PW 기반의 사용자 인증 기술보다 편의성을 향상 시키고 보안성을 증진 시킬 수 있을 것으로 기대된다.

본 논문은 2장에서는 관련기술을 3장에서는 보안성과 편의성을 향상시킨 인증 방식을 제안한다. 4장에서는 기존의 인증 방식과 비교 분석하여 제안한 방식에 대한 평가를, 5장에서 결론을 맺는 것으로 구성된다.

II. 관련 기술

1. 인증 개요

사용자는 정보 시스템에 접근하기 위해 사용자 인증을 통해 정당한 사용자임을 증명해야한다. 사용자 인증 시스템이 취약할 경우 해당 시스템은 해커의 공격 대상이 되어 기밀성, 무결성, 가용성이 침해되어 정보 시스템에 막대한 피해를 입히는 문제를 발생하게 된다.

즉, 취약한 인증시스템을 가진 정보시스템은 해커의 공격으로 인해 침해사고가 발생하게 되고 해커는 정당한 사용자의 권한으로 위장하여 시스템을 사용하게 됨을 의미한다.

2. 외부 기기(장치)를 활용한 사용자 인증[9]

2.1 이동저장매체(USB)[10]

이동저장매체(USB)를 활용한 사용자 인증 방식은 사용자의 PC에 전용 어플리케이션을 설치 후 사용자가 지정한 USB에 인증정보를 저장하는 방식 또는 전용 보안 USB에 인증정보를 저장하는 방식으로 나뉜다.

해당 방식은 PC에 인증정보가 남지 않으며, 전용 어플리케이션을 이용해 인증 정보를 재구성해 사용자가 비밀번호를 주기적으로 변경하지 않는 다는 장점이 있지만, 이동저장매체가 분실 또는 도난 되지 않도록 관리를 해야 한다는 번거로움과 이동저장매체가 없는 경우 인증을 진행 할 수 없어 상시적으로 소지해야 한다는 문제점을 가지고 있다.

2.2 스마트폰[11][12]

스마트폰을 활용한 사용자 인증 방식에는 스마트폰 또는 스마트폰 전용 어플리케이션을 이용한 자체 인증

방식과 스마트폰을 이용해 서버에서 인증을 받는 방식으로 나뉜다.

해당 방식은 스마트폰 사용자가 PIN코드, 비밀번호 패턴 락, 지문 등의 추가적인 방법으로 인증의 강도를 강화시킬 수 있다는 장점과 이동저장매체와 달리 사용자가 상시적으로 소지를 한다는 장점을 가지고 있지만 기기의 분실 또는 도난 되지 않도록 관리를 해야 한다는 번거로움과 보안정책 또는 분실로 인해 스마트폰을 사용하지 못하는 환경에서 인증을 진행할 수 없다는 문제점을 가지고 있다.

III. 제안 방안

본 논문은 사용자에게 친숙하며 범용적으로 쓰이는 ID/PW기반 인증 방식의 인증기술의 취약점과 스마트폰을 활용한 사용자 인증 방식에 초점을 두었다.

ID/PW기반 인증 방식의 가장 큰 취약점은 비밀번호의 유출인데 브루트 포스 공격, 키로깅, 스니핑과 같은 공격으로 인해 유출 될 가능성이 매우 높은 문제를 지닌다. 이에 대한 해결 방안으로 주기적으로 비밀번호를 변경하는 것이며, 한국인터넷진흥원(KISA)이 위탁 운영하는 '개인정보보호 종합포털'에서는 최소 6개월 마다 비밀번호를 바꿀 것을 권고하고 있다[13].

본 논문에서는 스마트폰이나 전용 PC 어플리케이션을 이용해 초기 등록을 하면 1회용 세션을 기반으로 비밀번호를 새로 생성해 주기적으로 비밀번호를 변경하지 않아도 보안성을 보장할 수 있는 사용자 인증 방안을 제안하였다. 사용자는 스마트폰 또는 전용 PC어플리케이션을 이용해 인증을 진행 할 수 있다. 또한 기존의 스마트폰 전용 어플리케이션을 이용한 인증 방안[14]의 문제점인 스마트폰이 반입 및 사용이 가능한 곳에서 밖에 사용할 수 없는 장소 제약성 문제와 인증정보를 기기에 가지고 보유하고 있어 기기의 도난이나 해킹으로 인해 인증정보가 탈취되는 문제점을 해결하기 위해 클라우드 서버를 사용하려고 한다. 등록 및 인증정보 재구성 과정에서 인증정보를 스마트폰이나 PC에 남기지 않고 클라우드 서버에 암호화하여 저장되어 기기의 분실 등으로 인해 발생하는 인증정보가 탈취 될 수 있는 문제를 해결하였다.

1. 시스템의 구조

본 절에서는 제안하는 인증 시스템의 구조와 동작 절차에 대해 설명한다. [그림 1]은 사용자 등록 및 인증을 수행하고, 인증정보를 클라우드에 저장하는 절차이며 각 단계의 세부 동작 절차는 다음과 같다.

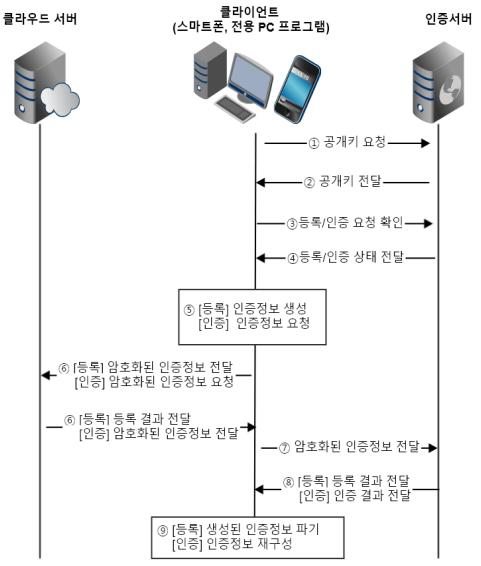

그림 1. 제안 시스템 구조

1.1 등록 절차

사용자가 정보시스템을 사용하기 위해서 서버에 사용자의 정보 등록을 수행하여야 한다. 등록 절차는 스마트폰/전용 PC 어플리케이션(이하, 전용 앱 이라고 한다.)에서 인증정보를 생성하여 인증서버와 클라우드 서버에 등록하는 과정이다. 클라이언트와의 모든 통신은 중간에 정보가 탈취되는 것을 방지하기 위해 SSL통신을 기반으로 하고 인증서버의 공개키(인증 서버의 공개키는 주기적으로 재발급한다.)를 이용해 인증정보를 암호화해서 클라우드 서버와 인증서버로 전송해 인증정보를 안전하게 저장한다. 등록 절차의 순서는 다음과 같다.

전용 앱에서 인증 서버의 공개키를 요청 송신 한다.

인증서버는 자신의 공개키를 전용 앱에 송신한다.

전용 앱에서 사용자의 인증 정보가 기존에 등록 되어 있는지 확인 요청을 송신한다.

사용자의 인증정보가 등록되어 있지 않은 경우 미등록 상태를 전용 앱으로 송신한다.

전용 앱이 설치된 기기에서 변경되기 어려운 고유한 값(MAC주소, 스마트폰:IMEI, PC: BIOS 시리얼넘버)과 time stamp 값을 가지고 인증정보를 생성 후 인증서버에서 수신한 공개키로 암호화하는 작업을 거친다.

전용 앱에서 기기의 고유 정보(MAC 주소)와 인증서버의 공개키로 암호화된 인증 정보를 클라우드 서버에 송신한다.

클라우드에서 DB에 암호화된 인증정보를 등록 후 결과를 전용 앱으로 송신한다.

등록 성공 시, 전용 앱에서 암호화된 인증정보를 인증서버로 송신한다.

인증서버에서 수신한 암호화된 인증정보를 서버의 개인키로 복호화 한 뒤, DB에 등록 후 결과를 전용 앱으로 송신한다.

등록 성공 시, 생성된 인증정보를 전용 앱에서 즉각 파기한다.

1.2 인증 절차

사용자가 정보시스템을 사용하기 위해선 사용자 인증을 수행해 정당한 사용자인지를 인증을 받아야한다. 인증 절차는 전용 앱 현재 사용자의 계정이 인증대기 상태중인지를 체크하고 인증대기 상태일 경우 클라우드에 사용자 기기에 귀속된 암호화된 인증정보를 조회하고 해당 인증정보로 인증을 수행하며, 인증이 정상적으로 완료되었을 경우 인증 정보를 재구성후 등록하는 과정이다. 인증 절차의 순서는 다음과 같다.

전용 앱에서 인증 서버의 공개키를 요청 송신 한다.

인증서버는 자신의 공개키를 전용 앱에 송신한다.

해당 사용자의 계정의 현재 상태 확인 요청을 송신한다.

인증요청 대기 상태인 경우 요청대기 상태임을 전용 앱으로 송신한다.

기기의 고유 정보(MAC주소)를 가지고 클라우드에 등록된 인증 정보를 요청한다.

전용 앱에서 해당 계정과 장치에 귀속된 사용자 인증정보 요청을 송신한다.

클라우드에서 DB에 있는 요청된 계정의 인증정보를 전용 앱으로 송신한다.

전용 앱에서 수신한 암호화된 인증 정보를 인증서버로 송신한다.

인증서버에서 수신한 암호화된 인증정보를 서버의 개인키로 복호화 한 뒤, 인증서버의 DB에 저장된 인증정보와 비교 후 인증 절차를 수행하며, 해당 결과를 전용 앱으로 송신한다.

전용 앱에 수신된 결과에 따라 인증정보 재구성 절차를 거친다.

1.3 인증정보 재구성

인증정보 재구성은 사용자 인증 절차가 정상적으로 이루어진 경우에만 진행하며, 전용 앱에서 사용자의 인증정보를 재구성한다. 해당 절차는 사용자 등록 절차에서 ⑤ ~ ⑩의 절차와 동일하다.

IV. 비교 및 분석

본 장에서는 ID/PW사용자 인증 방식, 지문 인증 방식, OTP인증 방식, 인증서 방식, 스마트폰 인증 방식, 제안방식과 비교 분석 하였으며, 내용은 [표 1]과 같다.

표 1. 인증요소 비교

	ID/PW	지문	OTP	인증서	스마트폰	제안 방식
특징	정적	정적	동적	정적	동적	동적
PW 변경	O	X	X	O	X	X
휴대성	높음	높음	보통	보통	보통	높음
장소제약	X	X	△	△	△	X
보안강도	낮음	높음	높음	높음	높음	높음
PW 기억	O	X	X	O	X	X
위변조 가능성	높음	낮음	낮음	낮음	낮음	낮음
재사용 방지	X	X	O	X	O	O
해킹가능성	높음	낮음	낮음	낮음	낮음	낮음

제안 방식은 일회용 세션기반 사용자 인증을 위해 사용되는 인증정보를 서버 사이드가 아닌 클라이언트 사이드에서 생성해서 사용자의 기기만의 고유한 값을 활

용해 사용자 기기가 아닌 타 기기에서 사용자 전용 인증정보를 재구성하기 힘들다는 점에서 ID/PW방식과 비교하여 해킹 가능성이 낮다고 할 수 있으며, 정적으로 인증정보를 생성하는 특징을 가진 ID/PW, 지문, 인증서 방식과 달리 제안 방식은 인증정보를 일회용 세션 기반으로 생성하는 특성을 가져 인증정보의 재사용을 방지한다. 또한 사용자의 기기(PC, 스마트폰)에 인증정보를 저장하지 않고 클라우드 서버에 암호화하여 저장한다는 점에서 위변조 가능성이 적고 기기에 인증정보를 저장하는 스마트폰 방식[12]와 달리 클라우드에 인증정보를 저장하여 사용자의 기기가 탈취되더라도 기기에 인증정보가 남아있지 않아 휴대성이 높고 장소제약을 받지 않은 장점이 있다.

V. 결론

최근 인증 방식은 ID/PW기반 인증 기술만을 이용한 사용자 인증을 진행하는 것이 아닌 2-factor인증 또는 Multi-factor을 조합한 ID/PW기반 사용자 인증을 진행한다[14]. 이 때 대부분 사용자들은 스마트폰의 어플리케이션을 이용해 추가적으로 PIN 코드나 OTP코드를 입력해 사용하지만 여전히 PW 탈취의 위험성이 있고, 스마트폰을 사용하지 못하는 환경이나 상황에서는 해당 인증 방식을 사용할 수 없게 되어 정보시스템에 접근하는데 어려움을 겪을 수 도 있다.

이에 본 논문에서는 기존의 ID/PW기반의 인증 방식에서 발생 가능한 PW탈취의 위험성과 스마트폰을 활용한 인증방식에서의 인증정보를 스마트폰 내부에 저장하는 방식 및 스마트폰을 사용하지 못하는 장소 제약성에 따른 문제 해결 방안으로 클라우드를 활용한 ID/PW기반 사용자 인증 강화 방안을 제안 하였다. 즉, 인증정보를 클라우드 서버에 저장하고, 필요 시 스마트폰 어플리케이션 또는 전용 PC 어플리케이션을 사용하여 MAC주소 인증절차를 인증을 진행 할 수 있도록 설계하였다.

[표 1]에서 비교분석한 내용과 같이 스마트폰을 활용한 인증 방법에 비해 휴대성이 더 좋으며 장소제약 또한 덜 받고, 일회용 세션을 기반으로 인증정보를 구성해 노출되어도 재사용이 불가능하며, 암호화되어 위변조와 해킹 가능성이 낮아 보안강도가 뛰어남을 알 수 있다.

이 논문에서 제안한 방식은 인증정보를 저장하는 클라우드 서버에 장애가 발생하였을 때 인증을 수행하는데 있어 어려움이 발생해 가용성이 하락할 수 있는 문제를 가지고 있다. 이러한 문제를 해결하기 위해서는 예비용 클라우드 서버의 추가적인 도입을 통해 가용성을 확보하는 방식이 있다. 각 클라우드 서버 간 데이터를 동기화 할 때 데이터의 무결성 및 최신 데이터 유지를 위한 방안에 대해 추가적인 연구를 진행하고, 향후 제안방식을 구현하여 실효성 및 성능에 대한 검증을 수행하고 구현하면서 논문에서 언급한 공격이 아닌 추가적으로 발생 가능한 공격들을 고려하여 대비가 가능할 수 있는 더욱 안전한 인증방식에 대한 연구가 필요하다.

참 고 문 헌

[1] https://m.blog.naver.com/PostView.nhn?blogId=2011topcit&logNo=220561565751

[2] https://www.boannews.com/media/view.asp?idx=72005

[3] http://www.itworld.co.kr/news/75363?page=0,1

[4] http://shindonga.donga.com/Series/3/990349/13/1479468/1

[5] http://www.nirs.go.kr/ncia_MJS/board/dev/board/board.jsp?id=data_202&cate=&key=subject&search=&order=&desc=asc&menu_num=3015&menu_num=3015&mode=view&pg=1&idx=2674

[6] https://msit.go.kr/cms/www/m_con/news/report/__icsFiles/afieldfile/2019/01/04/별첨 2. 4차 산업혁명 체감을 위한 클라우드 컴퓨팅 실행(ACT) 전략.pdf

[7] http://www.ddaily.co.kr/news/article/?no=181545

[8] www.itfind.or.kr/admin/getFile.htm?identifier=02-001-190104-000002

[9] 김선영, 김선주, 조인준, “이동 저장 매체를 활용한패

스워드 기반 사용자 인증 강화 방안," 한국콘텐츠학회 논문지, 제14권, 제11호, pp.533-540, 2014.
[10] 이진해, 김선주, 이진우, 조인준, "USB 메모리 장치 정보 및 암호를 기반으로 한 사용자 인증정보 관리방안," 배재대학교 공학연구소, 제18권, 제1호, pp.31-30, 2016.
[11] S. R. Na, S. Y. Shin, and T. K. Kwon, "모바일 ID를 저장하여 관리 및 이용하고 있는 스마트폰의 사용자 인증 동향," Jonornal of The Korea Institute of information Security & Cryptology, Vol.21, No.4, pp.22-31, Jun. 2011.
[12] 채영진, 이진우, 이진해, 조인준, "스마트폰을 이용한 ID/PW 기반 강화된 사용자 인승 시스템 설계," 배재대학교 공학 연구소, 제17권, 제1호, pp.35-41, 2015.
[13] https://www.privacy.go.kr/a3sc/per/chk/examInfoViewCQ4.do
[14] http://www.weeklypost.kr/news/articleView.html?idxno=161
[15] 김선주, "스마트폰 고유정보를 이용한 안전한 개인키 관리 방안," 한국콘텐츠학회논문지, 제16권, 제8호, pp.90-96, 2016
[16] 히로시 유키, *알기쉬운 정보보호개론 : 흥미로운 암호기술의 세계,* 인피니트북스, 2018.
[17] https://hn0110.tistory.com/374
[18] 김대현, *클라우드 컴퓨팅 환경에서 보안 강화된 개인 인증 시스템 설계 및 구현,* 가천대학교, 석사학위논문, 2013.
[19] 양새로미, *클라우드 환경 내 안전한 데이터 전송 및 활용 방안 연구,* 성신여자대학교, 석사학위논문, 2013.
[20] 김영곤, 김효종, 전문석, "기업에서 클라우드 컴퓨팅 사용을 위한 사용자 인증기법 연구", 한국정보과학회 학술발표논문집, 제37권, 제1호, pp.42-46, Jun. 2010.
[21] 정현미, *클라우드 컴퓨팅 환경에서의 효율적인 사용자 인증 설계 및 구현,* 한남대학교, 석사학위논문, 2010.

저 자 소 개

박 영 수(Yeong-Su Park) 준회원

- 2018년 2월 : 배재대학교 사이버보안학 학사
- 2018년 2월 ~ 현재 : 배재대학교 사이버보안학과 석사과정

〈관심분야〉 : 정보보안, 클라우드 컴퓨팅, 암호학, 네트워크 보안

이 병 엽(Byoung Yup Lee) 종신회원

- 1991년 2월 : 한국과학기술원 전산학과(공학사)
- 1993년 2월 : 한국과학기술원 전산학과(공학석사)
- 1997년 2월 : 한국과학기술원 경영정보공학(공학박사)
- 1993년 1월 ~ 2003년 2월 : 대우정보시스템 차장
- 2003년 3월 ~ 2016년 2월 : 배재대학교 전자상거래 학과 부 교수
- 2016년 3월 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 클라우드 컴퓨팅, 사용자 인증, 네트워크