Journal of Korea Multimedia Society Vol. 25, No. 9, September 2022(pp. 1284-1290)
https://doi.org/10.9717/kmms.2022.25.9.1284

고의적인 연속 인증실패에 대처하는 IP주소와 횟수 기반의 계정 잠금 방지에 관한 연구

정진호†, 차영욱††

A Study on IP Address and Threshold-based Account Lockout Prevention to Deal with Intentional Consecutive Authentication Failures

Jinho Jeong†, Youngwook Cha††

ABSTRACT

An attacker with a malicious purpose can intentionally type other users' accounts and passwords, causing them to be locked or revoked. Although NIST introduced methods to prevent this attack, all suggested methods are inappropriate to prevent an attacker from manually failing authentication, and reduce user availability. In this paper, in order to prevent user account lockout due to an attacker's intentional authentication failure, we propose a new authentication method using IP address and number of failed authentication. The proposed method not only blocks attackers who intentionally try to fail authentication, but also provides convenience to users because accounts are not locked or revoked. It can also safely protect passwords against password cracking attacks.

Key words: Account Lockout, Password, Authentication

1. 서 론

중요 웹사이트나 개인의 금융활동을 위해 국내에서는 공동인증서, 일회용비밀번호생성기(OTP), 생체인증 등을 활용하여 안전하게 인증한다. 발급사의 정책에 따라 사용자 인증 시, 비밀번호 인증이나 생체인증에 여러 번 실패할 경우 계정이 잠기거나 폐기될 수 있다[1]. 트위터, 마이크로소프트 등 전 세계 다양한 웹사이트에서도 이와 같은 인증방식을 사용중이다[2]. 악의적인 공격자는 기존 인증방식의 허점을 이용하여 인증을 고의적으로 실패하므로 사용자의 계정을 잠기게 하거나 폐기시킬 수 있다. 미국 국립표준기술연구소(NIST)의 Digital Identity Guidelines에서는 CAPTCHA, 30초에서 1시간 동안 재시도 금지, 요청했던 IP주소에 한해서 인증, 그리고 위치정보나 요청패턴 시간과 같은 사용자의 행위를 식별할 수 있는 방법들을 통하여, 고의적 인증실패 공격을 방지할 수 있다고 소개하였다[3].

그러나 NIST가 제시한 방법들은 연속 인증실패하는 공격을 근본적으로 막을 수 없는 취약점과 사용자를 제대로 식별하지 못하여 인증을 수행하지 못하는 문제점이 있으며, 사용자의 가용성을 저하시킨다. 본 논문에서는 공격자의 고의적인 인증실패를 차단하여 보안적으로 안전하고, 사용자의 계정이 잠기거나 폐기되지 않아 편의를 제공하며, 패스워드 크래킹으로부터 비밀번호를 안전하게 보호하는 새로운 인

※ Corresponding Author : Youngwook Cha, Address: (36728) 375, Gyeongdong-ro Andong-si Gyeongsangbuk-do, Republic of Korea, TEL : +82-54-820-5714, FAX : +82-54-820-6164, E-mail : ywcha@anu.ac.kr
Receipt date : Jul. 16, 2022, Approval date : Aug. 11, 2022.

† DJ FAMILY
(E-mail : jgw2846@naver.com)
†† Dept. of Computer Engineering, Andong National University
※ This work was supported by a Research Grant of Andong National University.

증방식을 제안한다.

본 논문의 2장에서는 계정이 잠기는 인증방식의 관련연구를 기술한다. 3장에서는 고의적인 인증실패 공격에 효과적으로 대처하기 위하여, IP주소와 횟수를 이용하는 새로운 인증방식을 제안한다. 4장에서는 제안한 인증방식의 구현과 안전성에 관한 내용을 기술하며, 5장에서는 결론 및 추후 계획에 대하여 기술한다.

2. 관련 연구

2.1 비밀번호 실패 시의 계정 잠김

2020년 6월 9일의 전자서명법 전면 개정에 의하여, 민간 전자서명 인증 사업자가 인증기관으로부터 증명서를 발급받아 전자서명 인증을 할 수 있게 되었다[4]. 이에 따라 공인인증서의 이름도 공동인증서로 바뀌었으며, 많은 민간기업에서도 인증서를 발급할 것으로 전망된다[5]. 공동인증서와 같은 인증도구들은 비밀번호를 통해 자격을 증명한다. 만약 일정 횟수 안에 인증되지 못할 시 인증서 혹은 계정이 잠기거나 폐기된다[1]. 인증서의 폐기가 전자서명법에 법으로 명시되지는 않았으나, 이는 보안을 안전하게 하기 위한 목적으로 보인다. 트위터, 마이크로소프트, 네이버, 인터파크 등 국내외의 다양한 웹사이트들도 비밀번호가 일정 횟수 틀리면, 계정이 잠기는 인증방식을 사용 중이다.

2.2 NIST의 디지털신원 가이드라인

인증실패로 인증서나 계정이 잠기면 다시 발급받아야 하는 번거로움이 있다. 미국 NIST의 디지털신원 가이드라인(Digital Identity Guidelines)에서는 제3자의 고의적인 연속 인증실패로 계정을 정지시키는 공격에 대비하는 기술을 제안하였다[3]. 금융보안원에서도 NIST의 제안을 인용하여 공문을 배포하였다[6]. NIST의 디지털신원 가이드라인에서 제안한 기술은 Table 1과 같다.

고의적 연속 인증실패를 방지하기 위하여 NIST는 첫 번째 기술로 CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)의 사용을 제안하고 있다. CAPTCHA는 대부분의 사람들이 통과할 수 있지만, 자동화 프로그램은 통과할 수 없는 테스트를 말한다[7]. CAPTCHA는 공격자가 사용자의 비밀번호를 알아내기 위하여 무작위 대입공격(Brute Force Attack)과 같은 공격을 자동화 도구로 사용할 때, 효과적으로 방어하는 용도로 적합할 수 있다. NIST의 두 번째 제안에서는 연속 인증실패 시에 30초에서 1시간 동안 재시도를 금지시키라는 것이다. 이 또한 자동화 도구를 이용한 공격 시에 인증시간을 지연 시킬 수 있다. NIST의 세 번째 제안은 화이트리스트에 있는 IP주소로부터 수신한 인증요청만 처리하는 것이다. NIST의 마지막 제안은 IP주소, 위치정보, 요청패턴 시간, 브라우저 메타데이터 등과 같이, 사용자의 행위를 식별할 수 있는 인증기술을 사용하는 것이다.

3. 고의적인 인증실패에 대처하는 IP주소와 횟수 기반의 인증

3.1 NIST 디지털신원 가이드라인의 취약점과 문제점

NIST가 제안한 4가지 방식의 취약점과 문제점은 다음과 같다. NIST의 첫 번째 제안인 CAPTCHA는 자동화 도구로 비밀번호를 크래킹하는 공격의 방어에 효과적이나, 공격자가 직접 CAPTCHA를 풀면서 고의적으로 비밀번호를 틀린다면 여전히 계정을 잠기게 하거나 폐기 시킬 수 있다. 두 번째 제안인 30초에서 1시간 인증 지연의 경우에, 공격자의 입장에서는 여전히 잘못된 비밀번호를 이용하여 고의로 인증실패를 유발할 수 있다. 공격자는 다른 계정의 실패

Table 1. NIST's intentional continuous authentication failure prevention technology.

Number	Technologies
1	Requiring the claimant to complete a CAPTCHA before attempting authentication.
2	Requiring the claimant to wait following a failed attempt for a period of time. (e.g., 30 seconds up to an hour)
3	Accepting only authentication requests that come from a white list of IP addresses.
4	Leveraging other risk-based or adaptive authentication techniques to identify user behavior. (IP address, geolocation, etc.)

를 만들면서 정해진 시간을 기다릴 수도 있다. 사용자가 실수로 비밀번호를 틀렸을 때 30초에서 1시간이나 기다려야 한다면 업무처리에 큰 제약이 될 수 있는 사용자 입장에서의 문제점도 있다. 세 번째 제안인 화이트리스트 방법은 모바일 기기와 같이 유동 IP로 인증하는 사용자에게는 문제가 될 수 있다. 동일한 모바일 기기로 인증함에도 IP주소를 동적으로 할당받는 경우에는 화이트리스트에 등록이 되지 않아 인증 요청이 수락되지 않는다.

네 번째 제안인 행위를 식별하는 인증기술 중에서 IP주소에 관한 인증은 세 번째 제안에서 나타나는 동일한 문제점이 적용된다. 위치정보로 행위를 식별하는 인증의 경우 한국에서만 인증하다가 해외에서 급하게 인증이 필요한 경우는 인증할 수 없게 되는 문제가 있을 수 있다. 요청패턴 시간으로 사용자를 식별할 경우 사용자의 요청시간이 불규칙하거나 시차가 있는 해외에서 인증을 시도할 경우에는 인증할 수 없게 될 수 있다. 사용자는 자신의 기기를 변경하거나, 혹은 불가피한 사정으로 다른 사람의 PC에서 인증을 시도할 수 있다. 이러한 경우에 브라우저 메타데이터로 사용자를 식별한다면, 인증을 할 수 없어 불편함을 초래할 수도 있다.

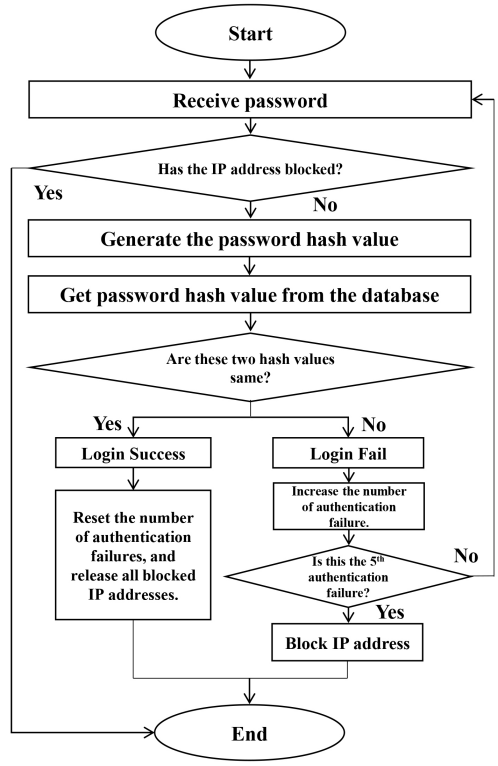


Fig. 1. Authentication procedure using IP address and failure number.

3.2 IP주소와 인증실패 횟수 기반의 인증방식

NIST가 제안한 방식은 연속 인증실패 공격을 근본적으로 막을 수 없는 취약점과 사용자를 제대로 식별하지 못하여 인증을 수행하지 못하는 문제점이 있으므로, 새로운 인증방식이 요구된다. 본 논문에서는 고의적인 연속 인증실패에 따른 사용자 계정의 잠금을 방지하기 위하여, IP주소와 인증시도 횟수를 이용하는 인증방식을 Fig. 1과 같이 제안한다. 제안한 인증방식은 고의적으로 인증을 실패하는 공격으로부터 안전하며, 사용자의 계정이 잠기거나 폐기되지 않아 사용자에게 편의성을 제공한다.

사용자가 비밀번호를 입력하여 인증을 시도하면, 사용자의 IP주소가 차단되어 있는지 검사한다. 해당 인증에 대하여 연속 5회 실패하는 경우에 인증을 시도한 단말기의 IP주소를 차단한다. 만약 사용자의 IP주소가 차단되어 있다면, 사용자가 입력한 비밀번호의 검증 없이 바로 인증실패 안내 페이지로 이동시킨다. 인증을 시도한 단말기의 IP주소가 차단되어 있지 않다면 사용자가 입력한 비밀번호를 시스템에 설정된 해쉬함수를 통하여 해쉬값을 만들고, 데이터베이스에 저장된 사용자의 비밀번호 해쉬값과 같은지 비교한다. 해쉬값이 다르면 인증을 시도한 사용자의 아이디와 IP주소를 데이터베이스에 등록시키고, 해당 사용자에 따른 IP주소의 인증실패 횟수를 1 증가시킨다. 연속해서 5번 인증실패 시에는 인증을 시도한 단말기의 IP주소를 차단하며 인증을 종료한다. 5번 미만인 경우에는 다시 인증을 시도하라는 오류 메시지를 표시하며 인증 페이지로 이동한다. 반면에 두 개의 해쉬값이 같다면 인증에 성공함을 나타내며, 해당 사용자의 인증에 실패했던 IP주소와 연관된 인증실패 횟수를 리셋 시킨다. 또한 인증에 성공한 계정과 연관되어 차단되어 있는 IP주소들도 모두 차단을 해제한다.

IP주소와 인증시도 횟수 기반의 인증방식은 공격자가 고의적으로 인증에 실패하더라도 사용자의 계정이 폐기되거나 잠기지 않는다. 정상적인 사용자가 실수로 계정의 비밀번호를 5번 틀린 경우에 해당 IP주소가 차단되더라도, 차단되지 않은 다른 IP주소의

기기에서 로그인 시도가 가능하며, 인증에 성공할 시에는 차단되었던 모든 IP주소 내역이 삭제되므로 원래 인증하던 기기에서 재인증이 가능해진다. 따라서 비밀번호를 알지 못하는 공격자는 사용자의 계정을 폐기시키거나 잠기게 할 수 없다. 또한 사용자의 비밀번호를 알아내기 위하여 무차별 공격을 시도하는 경우에도 5번 만에 비밀번호를 알아내지 못하면, IP주소들이 지속적으로 차단되어 비밀번호를 안전하게 보호할 수 있다.

4. 제안한 인증방식의 구현 및 안전성

4.1 제안한 인증방식의 구현 및 시험

Table 2는 인증서 혹은 계정의 비밀번호에 대한 인증실패 시에, 인증을 시도한 IP주소와 실패횟수를 저장하는 데이터베이스의 인증체크 테이블 구조를 나타낸다. AUTH_ID는 사용자의 계정 식별자를 나타내는 고유번호이다. FAILED_IP는 인증의 실패 시에 인증을 시도한 기기의 IP주소이며, IPv6에서는 콜론(:)을 포함한 주소의 최대길이가 39자리 이므로 VARCHAR(39)으로 지정하였다. COUNT는 인증에 실패한 FAILED_IP주소에 대하여 인증에 실패한 횟수를 나타낸다.

Fig. 2는 본 논문에서 제안한 인증방식을 최신버전인 PHP 8버전과 MySQL 8버전 환경에서 구현한 코드이다. 구현한 코드를 이용하여 제안한 인증방식의 실행여부를 시험하였으며, 기존 인증방식과의 실행시간을 비교하였다.

GetIpCheckedCount는 인증서 혹은 계정의 고유번호와 인증을 시도하는 기기의 IP주소를 입력받아 인증의 실패 횟수를 출력하는 함수이다. 5번 이상 인증이 실패한 IP주소, 즉 차단된 IP주소로는 해당 계정으로 더 이상 인증될 수 없도록 한다. 입력한 비밀번호의 해쉬값과 데이터베이스에 저장된 계정의 비밀번호 해쉬값이 일치하여 인증에 성공하면, 기존 실패했던 IP주소와 연관된 실패 횟수를 인증체크 테이블에서 삭제시킨 후 예정된 사이트로 이동한다. 인증에 실패하면 인증체크 테이블에 해당 계정과 IP주소의 내역이 없으면 SQL에서 INSERT 문을 실행시키고, 인증했던 내역이 있으면 UPDATE문을 실행시켜 인증실패 COUNT를 증가시킨다.

Table 3은 계정이 잠기거나 폐기되는 기존 방식과 본 논문에서 제안하는 방식의 처리 시간을 사용자의 비밀번호를 입력받은 때부터 인증의 완료 또는 실패 시점까지를 측정하였다. 계정이 잠기거나 폐기되는 횟수는 5번을 기준으로 잡았으며, 잠기거나 폐기되기 전, 잠기거나 폐기되는 시점, 잠기거나 폐기된 후, 그리고 인증에 성공했을 시의 시간으로 구분하여 측정하였다. 코드를 구현한 환경과 같은 PHP8 및 MySQL 8버전, 그리고 CPU 3.40GHz와 메모리 16GB DDR3 환경에서 측정하였으며, 항목 당 100회 측정의 평균을 기록하였다.

계정이 잠기거나 폐기되기 전의 경우에 기존 방식은 36ms, 본 논문에서 제안한 방식은 45ms로 측정되었다. 기존 방식이 약 9ms 빠르게 측정된 것은, 기존 방식에는 인증을 시도하는 IP주소가 5번 넘는 인증실패가 있었는지 확인하는 절차가 없기 때문이다. 계정이 잠기는 시점에서는 기존 방식이 56ms, 본 논문

Table 2. Database table structure for authentication procedure using IP address and failure number.

Column	Data Type	Contents
AUTH_ID	INT	Unique number of certificate or account
FAILED_IP	VARCHAR(39)	IP address for which authentication failed
COUNT	TINYINT	Number of failed authentication

Table 3. Performance comparison of existing method and proposed method.

Point	Existing method	Proposed method
Before locked or revoked point	36 ms	45 ms
At locked or revoked point	56 ms	45 ms
After locked or revoked point	10 ms	5 ms
Success point	5 ms	9 ms

```php
if(GetIpCheckedCount($auth, $ip) < 5)
{
    $password = "anul3579";

    // Fetch password hash value from DB
    $sql = "SELECT MEMBER_PASSWORD FROM member
            WHERE MEMBER_ID = '$auth' ";
    $rs = mysqli_fetch_array(mysqli_query($connect, $sql));

    // Check if user ID exists
    if($rs)
    {
        // Password hash value comparison
        if($rs['MEMBER_PASSWORD'] == hash('sha256', $password))
        {
            // Delete failed IP addresses and count
            mysqli_query($connect, "DELETE FROM authcheck
            WHERE AUTH_ID = '$auth'");
            mysqli_close($connect);

            header('Location: https://www.anu.ac.kr');
        }
        else
        {
            // Insert the failed IP address, and increase the number of failures
            mysqli_query($connect, "INSERT INTO authcheck
            (AUTH_ID, FAILED_IP, COUNT)  VALUES
            ('$auth', '$ip', 1)
            ON DUPLICATE KEY UPDATE
            COUNT = COUNT + 1");

            Alert("ID or Password is Wrong.");
        }
    }
    else
        Alert("ID or Password is Wrong.");
}
else
    Alert("You cannot authenticate with this IP address anymore.");
```

Fig. 2. Implementation of the proposed authentication method with PHP and MySQL.

의 방식은 이전과 같은 45ms로 약 11ms 빠르게 측정되었다. 본 논문의 방식은 인증에 5번 실패하더라도 인증실패 시마다 동일하게 IP주소를 등록 및 실패횟수를 1 증가시킬 뿐이지만, 기존 방식은 5번 실패 시 해당 계정을 잠기게 하거나 폐기시키는 절차가 있기 때문이다. 계정이 잠긴 후의 경우에 본 논문의 방식은 5ms로 기존 방식의 10ms보다 5ms 빠르게 처리되었다. 기존 방식은 해당 계정의 존재 유무와 잠김 혹은 폐기 여부를 검색하는 절차가 있는 반면, 본 논문의 방식은 단순히 IP가 차단되었는지 만을 확인한다. 마지막으로 인증에 성공한 경우에 기존 방식은 5ms이며, 본 논문의 방식은 9ms로 기존방식이 약 4ms 빠르게 처리되었다. 기존 방식은 인증에 성공 시 인증완료 페이지로 바로 이동하지만, 본 논문에서 제안한 방식은 인증완료 페이지로 이동하기 전에 모든 실패 기록을 삭제하는 절차가 있기 때문이다. 본 논문의 방식은 기존 방식에 비해 편의성이 크게 증대되었으며, 계정의 잠김 시점과 잠김 후에는 인증처리 시간도 각각 11ms, 5ms 빠르게 처리되었다. 계정이 잠기기 전과 인증성공 시의 경우에는 본 논문의 방식이 기존 방식에 비해 각각 9ms, 4ms의 시간이 추가되었다.

4.2 제안한 인증방식의 안전성과 편리성

KISA의 패스워드 선택 및 이용 안내서는 알파벳 대문자와 소문자, 특수문자, 숫자 중 두 종류 이상의 구성과 8자리 이상의 문자열을 안전한 비밀번호로 권고하고 있다[8]. 이에 따라 인증서 및 중요 인증을 위한 계정은 해당 비밀번호 가이드를 따르고 있다. 영문 대소문자와 숫자의 조합으로 8자리 비밀번호를

만든다고 가정하였을 때, 비밀번호의 모든 경우의 수는 62의 8제곱으로 218,340,105,584,896이다.

한 개의 IP주소 당 5번까지 시도가 가능하다면, 8자리 비밀번호를 찾아내기 위해 필요한 최대 IP주소의 개수는 약 43,668,021,116,979 (=218,340,105,584,896/5) 개이다. IPv4 기준 나올 수 있는 최대 IP주소의 개수는 이론상 2의 32제곱인 4,294,967,296개이며, 이는 8자리 비밀번호를 찾아내기 위해 요구되는 최대 IP주소의 개수보다 훨씬 적은 1/10,000 수준이다. 제안한 인증방식에서는 5번 인증에 실패하면 인증을 시도한 기기의 IP주소가 차단되므로, 모든 IP주소를 가지고 무작위 대입공격을 한다고 해도, 공격자가 소유하고 있는 모든 IP주소가 차단될 때까지 사용자의 비밀번호를 크래킹할 확률은 매우 낮다. 그러므로 제안한 인증방식이 IPv4 망에서 공격자의 패스워드 크래킹 공격에 매우 높은 안전성을 보장할 수 있다.

Table 4는 5회 연속으로 인증실패 시 계정이 잠기거나 폐기되는 기존 방식과 NIST에서 제안한 방식, 그리고 본 논문에서 제안한 방식을 편리함과 보안 그리고 크래킹을 위해 요구되는 IP주소의 수를 정리한 것이다. 기존 방식과 NIST 방식은 모두 5회 연속으로 인증실패 시에 계정이 잠기거나 폐기되어 사용자에게 불편함을 초래한다. 반면, 본 논문에서 제안하는 방식은 인증에 실패하여도 계정이 잠기거나 폐기되지 않아 사용자에게 불편함을 주지 않는다. 계정이 잠기거나 폐기되는 측면에서의 보안은, 기존 방식과 NIST 방식 모두 고의적인 인증실패 공격을 받게 되면 계정이 폐기되거나 잠기게 된다. 본 논문에서 제안한 방식은 고의적으로 인증을 실패하는 공격자의 IP주소를 차단하지만 계정이 잠기거나 폐기되지는 않는다.

공격자가 사용자의 비밀번호를 알아내기 위해 필요한 IP주소의 개수는, 기존 방식과 NIST 방식 모두 IP주소의 개수와 상관없이 5회 연속으로 인증실패 시 계정이 잠기거나 폐기된다. 사용자의 계정을 잠기게 하거나 폐기시키는 측면에서 보안적으로 뛰어나 보이지만, 잠긴 계정을 풀어야하는 사용자의 측면에서는 매우 불편하다. 또한 고의적인 인증실패 공격으로 계정이 폐기된다면, 정보보안의 3대 요소[9] 중 가용성이 매우 떨어지므로 보안이 좋다고 할 수 없다. 본 논문에서 제안한 방식은 사용자의 계정을 잠기게 하거나 폐기하지 않아 사용자의 가용성이 저하되는 상황은 발생하지 않게 된다. 또한 공격자가 비밀번호를 크래킹하기 위하여 비밀번호 8자리 기준 최대 43,668,021,116,979개의 IP주소가 필요하다. 미국 보안전문업체 Imperva 연구원에 의하면, 전 세계 많은 사물 인터넷(IoT)를 감염시키고 대규모 분산서비스거부 공격(DDoS)을 일으켰던 미라이 봇넷은 약 49,657개의 고유 IP주소를 감염시켰다고 한다[10]. 미라이 봇넷이 확보한 49,657개의 IP주소는 8자리 비밀번호를 알아내기 위한 IP주소 개수, 43,668,021,116,979개 보다 훨씬 적은 수이다. 이처럼 공격자가 확보할 수 있는 IP주소의 개수가 기껏해야 수만에서 수십만 개이므로, 본 논문에서 제안한 인증방식은 비밀번호 크래킹 공격으로부터 안전성을 보장할 수 있다.

5. 결 론

본 논문에서는 공격자의 고의적인 인증실패로 발생하는 사용자 계정의 잠김을 방지하기 위하여, 인증에 실패한 IP주소와 시도 횟수를 이용하는 새로운 인증방식을 제안한다. NIST에서 제시한 방법들은

Table 4. Comparison of existing, NIST and proposed authentication methods.

	Existing authentication method	NIST authentication method	Proposed authentication method
Convenience (In the case of authentication failure 5 times in a row)	Account is locked or revoked.		Account is not locked or revoked
Security (In the case of intentional authentication failure by attacker)	Attacker can lock a user's account.		Account can't be locked or revoked
Number of IP addresses required for password cracking (Password length is eight)	Regardless of the number of IP addresses, account is locked or revoked when authentication fails 5 times in a row.		In the worst case, 43,668,021,116,979 IP addresses

연속 인증실패하는 공격을 근본적으로 막을 수 없는 취약점과 사용자를 제대로 식별하지 못하여 인증을 수행하지 못하는 문제점이 있으며, 사용자의 가용성을 저하시킨다.

본 논문에서 제안한 방식은 인증할 계정에 동일한 IP주소로 5번까지만 인증시도가 가능하다. 5번 안에 인증에 성공하지 못하면 해당 IP주소를 차단하며, 차단된 주소로는 더 이상 인증을 진행할 수 없게 된다. 만약 인증에 성공하면, 해당 계정의 실패 횟수뿐 만 아니라 차단되었던 IP주소를 모두 해제한다. 이는 고의적으로 인증을 실패하는 공격자를 차단하여 계정을 안전하게 보호하지만, 해당 계정을 잠그거나 폐기하지 않아 사용자에게 편의성을 제공한다. 만약 사용자가 실수로 5번 모두 인증에 실패하여도 다른 기기를 통해 인증에 성공하면 차단된 IP주소가 해제되므로, 원래 인증해왔던 기기에서 다시 인증이 가능해진다. 본 논문에서 제안한 방식은 기존 방식에 비해 편의성이 크게 증대되었으나, 인증실패 전 인증 시도와 인증성공 시에 처리시간이 각각 9ms와 4ms 증가에 불과하였으며, 계정의 잠김 시점과 잠김 후에는 기존 방식보다 11ms와 5ms 빠르게 처리되었다. 또한 공격자가 확보할 수 있는 IP주소 개수에 한계가 있으므로, 제안한 인증방식은 공격자의 패스워드 크래킹 공격으로부터 비밀번호를 안전하게 보호할 수 있다.

본 논문에서 제안한 인증방식은 공격자의 고의적인 인증실패에 효과적으로 대처하며, 패스워드 크래킹에도 안전성을 보장하므로, KISA의 패스워드 선택 및 이용 안내서[8]에 권고사항으로 지정되도록 제안할 예정이다.

REFERENCE

[1] e-SAFE, https://e-safe.ksd.or.kr/page/signCenter/lock.jsp (accessed July 10, 2022).

[2] Twitter, https://help.twitter.com/en/managing-your-account/locked-out-after-too-many-login-attempts (accessed July 10, 2022).

[3] National Institute of Standards and Technology (NIST), *Digital Authentication Guidelines Authentication and Lifecycle Management*, NIST Special Publication 800-63B, 2017.

[4] Ministry of Science and ICT, *Electronic Signature Act*, 2021.

[5] Korea Policy Briefing, https://www.korea.kr/news/reporterView.do?newsId=148880719 (accessed July 10, 2022).

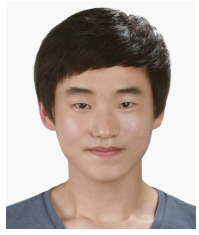
[6] Financial Security Agency, NIST, *Recommendations on Password Management*, 2021.

[7] N. Roshanbin and J. Miller, "A Survey and Analysis of Current CAPTCHA Approaches," *Journal of Web Engineering*, Vol. 12, pp. 1-40, 2013.

[8] Korea Internet & Security Agency (KISA), *Password Selection and Usage Guide*, 2019.

[9] T. Keyser and C. Dainty, *The Information Governance Toolkit: Data Protection, Caldicott, Confidentiality (1st ed.)*, CRC Press, 2005.

[10] SecurityWeek, https://www.securityweek.com/mirai-botnet-infects-devices-164-countries (accessed July 10, 2022).



정 진 호

2019년 안동대학교 컴퓨터공학과 (공학사)
2021년 안동대학교 컴퓨터공학과 (공학석사)
2021년~현재 안동대학교 컴퓨터공학과 대학원
2015년~현재 디제이패밀리 대표
관심분야 : 웹보안

차 영 욱

1987년 경북대학교 전자공학과 (공학사)
1992년 충남대학교 전자통계학과 (공학석사)
1998년 경북대학교 컴퓨터공학과 (공학박사)
1987년~1999년 한국전자통신연구원 선임연구원
2003년~2004년 매사추세츠주립대학 방문학자
2019년~현재 안동대 사이버보안 센터장
1999년~현재 안동대학교 컴퓨터공학과 교수
관심분야 : 망/시스템 제어 및 관리, 블록체인 및 보안, 개방형통신망