Applying MAC Address-Based Access Control for Securing Admin's Login Page

Bintang Maulana Prasetya Pagar Alam, Rycka Septiasari, and Amiruddin Amiruddin
Cyber Security Engineering, Sekolah Tinggi Sandi Negara
Bogor, Indonesia
{bintang.maulana, rycka.septiasari}@student.stsn-nci.ac.id, amir@stsn-nci.ac.id

***Abstract*—Authentication is a very important process for securing web applications. Username and password are two parameters commonly used for user authentication on the administrator's login page. However, such the two authentication parameters can be easily breached so that they can become a vulnerability that adversary parties can use to conduct malicious activities. For example, the attackers can commit a crime such as data modification or theft or even more dangerous take over administrator services of a system. Therefore, it is necessary to improve the security mechanism by adding additional factor of authentication other than username and password. In this study, an improvement in authentication mechanisms was carried out by applying MAC Address-based access control as an additional authentication factor. In this method, Address Resolution Protocol (ARP) is used in mapping the users Internet Protocol (IP) address to their MAC address during validation process. The experimental results showed that the addition of the MAC address made the authentication process resistant to Dictionary Attack and Shoulder Surfing Attack.**

Keywords—Administrator, Authentication, Dictionary attack, Login, MAC Address, shoulder surfing

I. INTRODUCTION

The administrator's login page on the web application is very important since it is the entry point to the whole system. Login pages that are not secured greatly endanger data and information in web applications. Authentication is one of the most important method for web security [1][2]. Username and password are two parameters commonly used for two-factor authentication on the admin's login page. However, the two authentication parameters can be breached so that it becomes a vulnerability gap that malicious activities. For example, attackers can use it to commit a crime such as data modification or theft or even more dangerous to take over the administrator services of a system. Therefore, it is necessary to improve the authentication mechanism on the admin's login page by adding additional factor [1][2] other than username and password.

The login process on admin's page consists of three stages i.e. identification, authentication and authorization [3]. The admin's login page functions to serve all the three stages for users to access the system that can only be accessed by the true admins and not the malicious ones. The identification process is done by checking the user's username, whether it has been registered in the user's database. Next, the authentication process is done by comparing the password entered by the user with the password stored in the database. Finally, the authorization process is done by checking the status of the user's access rights to resources. For short term, all the three stages is commonly called authentication.

In this study, we proposed an application of MAC address as an additional parameter to improve the security of the authentication mechanism. Address Resolution Protocol (ARP) is used in mapping the user's IP Address to the MAC Address in the validation process. The use of MAC Address as an authentication parameter aims to increase the security of the web applications. If the username and password are stolen / known by unauthorized parties, they can not use it on the admin's login page without true MAC address. The idea was that MAC Address varies on each device that makes it unique and has the potential as an authentication factor. To enter a system as an administrator, a user required to use a device with registered MAC Address. In this case, the use of the MAC Address as an access control on the admin's login page can be implemented on the internal network.

.

II. RELATED WORKS

In the literature, there are several research results that propose an authentication solution to log into a website. Lupu [4] introduced a real time, multi-factors authentication method using voice calls generated by a one-time password for web server communication. Haekal et al. [5] implemented an authentication method based on the token, JSON web token, for securing the process of authentication on a multi-platform web service called SIKASIR. Varshney et al. [6] analyzed several authentication schemes for identifying their vulnerabilities and proposed a secured authentication scheme for user identification. The scheme which uses Bluetooth Low Energy (BLE, BT 4.0+ Version) device can handle Real-Time (RT) / Control Relay (CR) Man in The Middle attack (MITM) phishing attack. Takamizawa [7] proposed a user authentication method for an e-learning system using topographical information from Google Maps. Morii et al. [8] proposed an integrated authentication system without the use of password, adopting Fast Identity Online (FIDO), as an external authentication technique. Dubey et al. [9] proposed a hybrid model, where fingerprint authentication is used with auto-complete function for accessing a specific website or information on the website. In that method, when certain pre-configured rules are met, the fingerprint module is triggered automatically.

In this study, we proposed an authentication method based on the MAC address for accessing the admin's login page.

III. Research Method

This study used experimental method [10], a method commonly used to compare the conditions of the subject before being treated and after being treated. The treatment carried out in this study is the implementation of MAC Address Access Control on the administrator login page. The idea of implementing the MAC address in this study is given in Figure 1 with the following explanation. The security of an administrative login page that only uses a username and password can be broken if the password is leaked. So, it is needed to add another parameter for authentication on the login page. In this study, the additional parameter is MAC address. After MAC Address implementation, a serial test is carried out on the login page with a simple dictionary attack and shoulder surfing attack scenario.

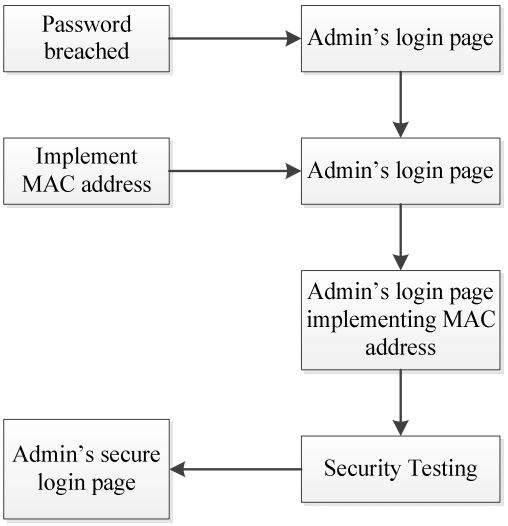

Figure 1. Implementation idea

The flow of the MAC address implementation for authentication on the login page is given in Figure 2. After being on the login page, the admin enters a username and password. Then the system checks the MAC address of the admin. If the MAC address does not match, the access request is denied. If the MAC address is appropriate, continue checking the username and password. If the username and password match then access is granted and otherwise access is denied.

The attack simulation in this study was done by dictionary attack and shoulder surfing attack and the flow of the attacks is given in Figure 3. In the dictionary attack, a list of alleged usernames and passwords will be created in the login form to try the security system whether it is successful or not. Dictionary attack was done by using Burp suite tools [https://portswigger.net/burp]. If the condition is true, it will continue to the username and password validation. Then if the username and password are valid, it will continue to the administrator web page. And if the condition is not true, the process will be repeated from the login page.

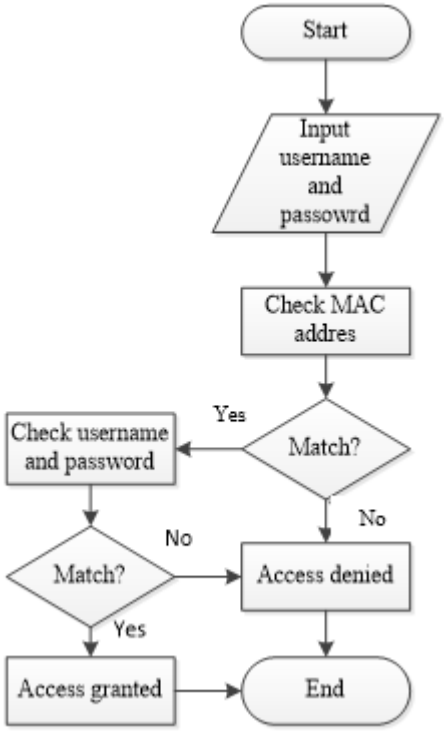

Figure 2. Flow of the system

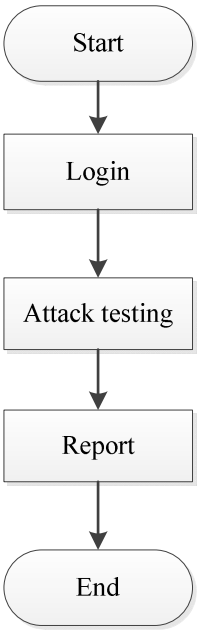

Figure 3. Attack testing flow

IV. Result and Discussion

A. Analysis of MAC Address work

In making an information system it is necessary to create a user-friendly and interactive interface to make the users feel convenient. The login page interface the proposed application is shown in Figure 4.

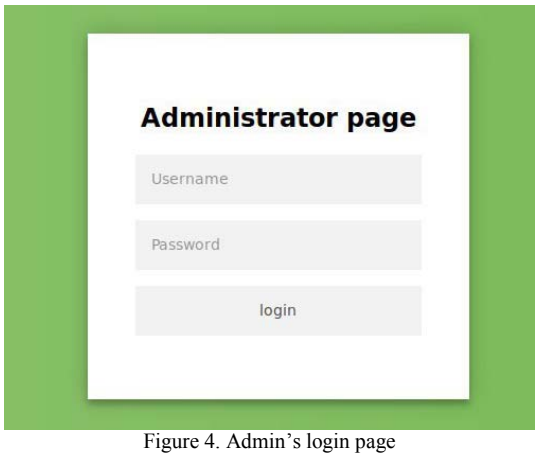

Figure 4. Admin's login page

The following is the script using PHP for implementing the Admin's login page without HTML.

```
<?php

$ip = $_SERVER['REMOTE_ADDR'];
#echo "$ip<br>";
ob_start();
system("arp -a $ip");
$arp= ob_get_contents();
ob_clean();

$mac = $arp[21].$arp[22].$arp[23].$arp[24].$arp[25].$arp[26].$arp[27].
$arp[28].$arp[29].$arp[30].$arp[31].$arp[32].$arp[33].$arp[34].$arp[35].
$arp[36].$arp[37].$arp[38];

$mac1 = sha1($mac);
$servername = "localhost";
$user = "root";
$sandi = "kamsiberstsn";
$database = "project";
$conn = mysqli_connect($servername, $user, $sandi, $database);
$username = $_POST["username"];
#$username = filter_var($username,
FILTER_SANITIZE_SPECIAL_CHARS);
$password = sha1($_POST["password"]);
$masuk = "select * from akun where username='$username' &&
password='$password'";
$login = mysqli_query($conn, $masuk);
$result = mysqli_num_rows($login);

if($username){

        if ($mac1 ==
"31e9ac605b95d5c5111e3d2218cfc7a3f71b9617"){

                if($result > 0){
                        $user = mysqli_fetch_array($login);
                        session_start();
                        $_SESSION["username"] =
$user["username"];
                        header ("location: ../index.html");
                                echo "<script>alert('Access
Granted')</script>";

                }
                else {
                                echo "<script>alert('Access
Denied')</script>";
                }
        }
        else{
                echo "<script>alert(' Access Denied ')</script>";
        }
}
```

In this experiment, the admin is a superuser. Admin can change, add, delete, and process data on information system or a website-based application. Attacker will try to by-pass to become an administrator on the information system or web-based application so that the attacker has access to the system as an administrator. The way that an attacker does was launch a dictionary attack and shoulder surfing attack.

Detection of MAC Address

In conducting the detecion of MAC address, the server uses ARP table for verifying the corresponding IP Address with the MAC address. The script used for conducting detection of MAC address is as follows.

```
<?php

$ip = $_SERVER['REMOTE_ADDR'];
#echo "$ip<br>";
ob_start();
system("arp -a $ip");
$arp= ob_get_contents();
ob_clean();

$mac =
    $arp[21].$arp[22].$arp[23].$arp[24].$arp[25].$arp[26].$arp[27].$ar
    p[28].$arp[29].$arp[30].$arp[31].$arp[32].$arp[33].$arp[34].$arp[3
    5].$arp[36].$arp[37].$arp[38];

echo $mac."<br>";
echo sha1($mac);
```

In detecting the IP address, the system can use the function of $_SERVER in PHP. Using the fucntion many keys can be applied. One of them is key ['REMOTE_ADDR'] which is useful for displaying the IP address of client accessing the website.

```
$ip = $_SERVER['REMOTE_ADDR'];
```

The results displayed from this source code are the client's IP Address that will be stored in the $ ip variable. In connecting website with the webserver to view ARP tables, **system ()** function in PHP was used. This function is useful for the server to execute input queries. To see the ARP table, the query "arp -a" was used. In the ARP table, there is an IP Address and MAC Address of the client so that this query will display the entire MAC Address of the client.

```
system("arp –a $ip");
```

The results of using the **system** () function will be immediately displayed without the **echo** function. This is different from the use of variables that require buffers to store results before they are displayed. To open the buffer in PHP, the **ob_start ()** function was used and to delete the contents of the buffer, the **ob_clean ()** function was used.

```
$arp = ob_get_contents()
```

The **ob_get_contents()** function is useful for entering the contents of the buffer into the $ arp variable which will be used to detect the client's MAC Address. From the results displayed when executing "arp -a $ ip", the MAC Address was in the 21st array to the 38th array.

```
$mac = $arp[21].$arp[22].$arp[23].$arp[24].$arp[25].$arp[26].$arp[27].$arp[28].$arp[29].$arp[30].$arp[31].$arp[32].$arp[33].$arp[34].$arp[35].$arp[36].$arp[37].$arp[38];
```

For adding confidentiality, the hash value of the $mac content was calculated using function **sha1()** in PHP as the following script.

```
sha1($mac);
if ($mac == 31e9ac605b95d5c5111e3d2218cfc7a3f71b9617){
[funtion when successful]
}
Else{
[function when failed]
}
```

The hash value of each detected MAC address will be calculated and then compared with the true hash value.

B. Analysis of attacks testing

In this experiment there were 2 (two) users namely administrator and attacker. The MAC address of the administrator was ac: d1: b8: 83: 6f: cf with username and password of the administrator was “rycka” and “rycka”, respectively. The attacker's MAC Address was 08: 00: 26: fc: 6f: 07. In this experiment, we used two attacks scenario, dictionary attack, and shoulder surfing.

In the first scenario, the dictionary attack, the attacker tried to log in to the admin’s web page using a list of passwords with username “rycka”. In the second scenario, the shoulder surfing attack, it is assumed that the attacker was already known the username and password. Therefore, the attacker tried to enter the known username and password for logging in to the admin’s web page. As shown in Figure 6, the attacker failed to log in as an administrator, because the device used to access the login page is different from the device used by the administrator.

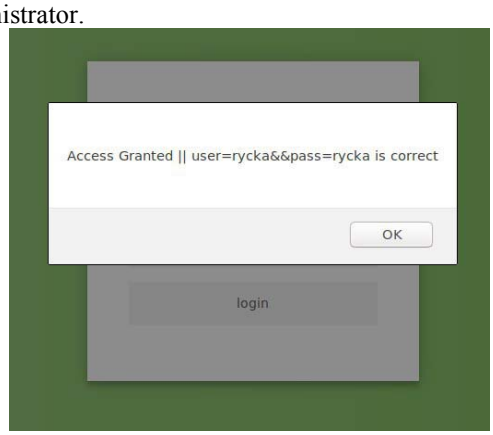

Figure 5. Succeeded login as an administrator

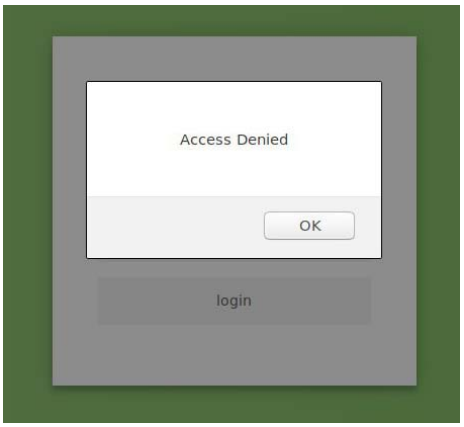

Figure 6. Failed login as an administrator

The following is the description of the proof of the attack scenario used in this experiment.

1. Dictionary attack

In carrying out this attack, the attacker managed to get a username that is "rycka", but the attacker is not known the password of the admin.

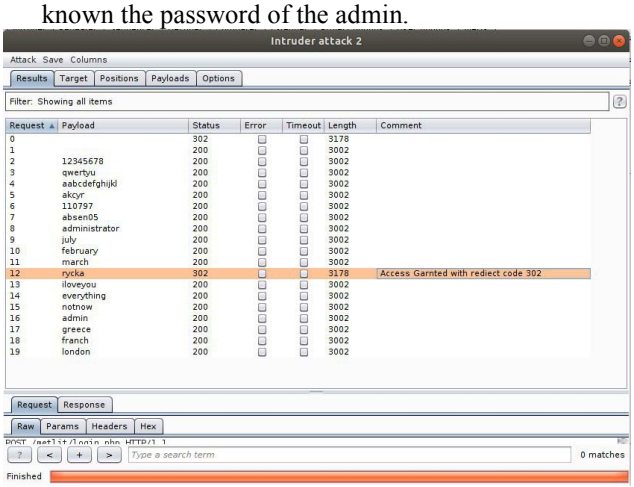

Figure 7. Dictionary attack testing without implemented MAC Address

Figure 7 shows the results of a dictionary attack using the Burp Suite. When the experiment used administrator login page without additional security in the form of MAC Address, the attacker successfully obtained the true password "Rycka" and the attacker was successfully redirected to the administrator page with a 302 redirect page code.

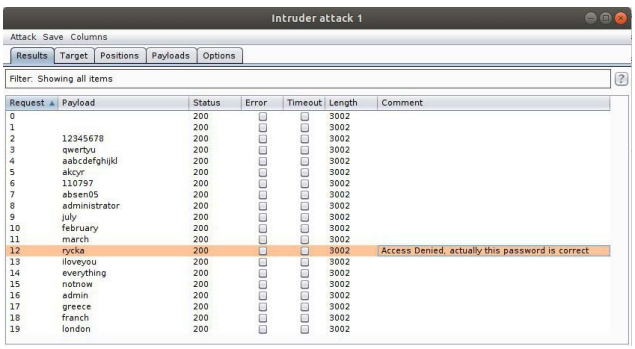

Figure 8. Dictionary attack testing with implemented MAC address

Figure 8 shows the results of a dictionary attack using the Burp Suite. In that experiment, we used the administrator login page with additional security in the form of MAC Address. Even though it successfully obtained the true password, the attacker did not succeed in accessing the administrator page, indicated with a code of 200 success loading pages. The attacker just got the administrator's login page and could not enter the admin's web page, because the MAC address on the attacker's device used was not valid [11].

2. Shoulder surfing attack

In this experiment, a dictionary attack was considered a failure to attack the administrator's page, then the attacker did shoulder surfing attack and found that the administrator's username and password are "rycka" and "rycka". The attacker tried to log in using tools **curl** as shown in Figure 9. From the results obtained, the password obtained from the shoulder surfing attack was also failed to gain access to the administrator web page.

```
$ curl -data \
"username=rycka&password=rycka" \
http://192.168.0.149/project/login.php
```

```
<script>alert('Access Denied')</script>
```

Figure 9. The result of Shoulder Surfing Attack.

V. CONCLUSION

In this research, an access control experiment has been carried out by applying a MAC Address and conducting a system test with a simple attack scenario, dictionary attack and shoulder surfing attack. From the result of design, experiment, and tests, it can be concluded that the application of the MAC address as an additional authentication parameter on the administrator's login page can increase security on the administrator page. In this experiment, it was found that the administrator login page without the application of MAC address was more resistant to dictionary and shoulder surfing attacks compared to that with application of MAC Address in the authentication process. In the attack test, the attacker can still get the admin's password and username, but the two authentication parameters were not enough to log in as an administrator because the MAC address used by the attacker is different from the registered MAC address of the admin.

REFERENCES

[1] K. Scarfone, W. Jansen, and M. Tracy, "Guide to general server security," 2008.

[2] J. IT Security Center (ISEC) Information Technology Promotion Agency, *How to Secure Your Website*. 2011.

[3] S. Bryan and L. Vincent, *Web Aplication Security*. New York: Mc Graw Hill, 2012.

[4] V. Lupu, "Securing Web Accounts by Graphical Password and Voice Notification," *2018 IEEE Int. Conf. Eng. Technol. Innov. ICE/ITMC 2018 - Proc.*, 2018.

[5] M. Haekal and Eliyani, "Token-based authentication using JSON Web Token on SIKASIR RESTful Web Service," *2016 Int. Conf. Informatics Comput. ICIC 2016*, 2017.

[6] G. Varshney, M. Misra, and P. Atrey, "A new secure authentication scheme for web login using BLE smart devices," *Proc. Int. Conf. Anti-Counterfeiting, Secur. Identification, ASID*, 2018.

[7] H. Takamizawa and N. Tanaka, "User authentication method using topographical information of google maps," *Proc. 2012 Int. Conf. Green Ubiquitous Technol. GUT 2012*, 2012.

[8] M. Morii *et al.*, "Research on Integrated Authentication Using Passwordless Authentication Method," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 1, 2017.

[9] U. Dubey, A. Trisal, J. Bose, M. Brabhui, and N. Ahamed, "A hybrid authentication system for websites on mobile browsers," *Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014*, 2014.

[10] Y. Kumar S., *Fundamental of Research Methodology and Statistics*. New Delhi: New Age International, 2006.

[11] S. W. Richard, *TCPIP Illustrated*, 2nd ed., vol. 1. Pearson Education, 2012.