A Practical Mechanism for Password Change of Multiple Systems in an Organisational Setting

Ruhi Taş*, Özgür Tanrıöver*

* Department of Computer Engineering, Faculty of Engineering, Ankara University, Gölbaşı 50.yıl Yerleşkesi Bahçelievler Mah. 06830, Gölbaşı/Ankara/Turkey
‡ Gölbaşı 50.yıl Yerleşkesi Bahçelievler Mah. 06830, Gölbaşı/Ankara/Turkey Tel: +90 312 463 3967, Fax: +90 312 463 4007, e-mail: ruhitas@yahoo.com

Abstract- Security policies force to clients frequently to change their password. This is particularly an issue for organisation with different administrations which require to access applications. In this paper, we propose a functional and minimal effort verification application that lessens client reliance to reset and confirm client for clients' password change on multiple sites. The proposed arrangement does not require any extra equipment for achieving new password immediately to access to organisations. The proposed framework includes utilizing a cellular telephone as a SMS based framework with checking password policy according to cloud based citizen info web service.

Keywords- Access Protocol, Password change, Domain Controller, LDAP, Brute Force

1. Introduction

Resources accessible through the web include a large number of private, open, scholastic, business, and taxpayer supported organizations. Every one of these service applications require username and password. Whether it is controlling access to organization assets, for example, Web Servers (email, FTP and so on.) - Web Customer (program) correspondence and all applications requires a password. While the web based system offers us numerous advantages, there is likewise a scope of wellbeing and security dangers connected with its utilization. One of the most vital difficulties is to guarantee security in these sites. Password confirmation is one of the least complex and long term verification systems over unreliable systems. It helps to authenticate clients to utilize the assets of the remote systems.

Passwords aren’t completely unbreakable, but they can keep culprits from getting to access rights of your systems. The vast majority of people use simple to-recall passwords in the system situations. In any case, those feeble passwords are inclined to brute force reference attacks [1]. One-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. OTP systems take care of password security issue that can happen by rehashing the same password a few times for various frameworks [2, 3]. Still, the usage of OTP systems might be expensive or need extra effort to manage it.

Another related issue is that, organizations are using many of different application for news production and other purposes. Such as FTP system, news management, electronic document management, graphics automation, advertisement management systems etc. Each of them has different passwords for different activities and changes them regularly, especially those for sensitive exchanges, for example, managing an account, long range informal communication and staff PC.

In this study, we have built up a viable and low-cost confirmation application that decreases client reliance to reset and create clients’ password when
critical timely access is required. The proposed solution does not require additional hardware for producing new password. The proposed system involves using a mobile phone for SMS based system for password generation.

2. Background and Related Methods

Recently, many studies about on cryptography and security password administration have been conducted. A generally accepted secure login technique depends on the token or smart card. ISO/IEC 7816 is a series of International Standards specifying these smart cards and the use of such cards for interchange. These cards are identification cards intended for information exchange negotiated between the systems and the integrated circuit in the card. As a consequence of a data exchange, the card transfers data and/or changes its value [4, 5]. This technique gives strong confirmation method with password verification, but it can be lost or stolen. It can be problem to carry them all times [6] OTP creation strategies; to start with, S/key strategy, second the test reaction technique, and time-synchronous strategy where the executive sets a timeframe when the password is valid [7, 8].

The OTP authentication system uses computation technique to generate a sequence of single-use passwords from a single secret. OTP tokens are usually pocket-size fobs with a small screen that displays a number. The number changes every 30 or 60 seconds, depending on how the token is configured. All the security is entirely based on a single secret that is known only by the user [9]. The user enters his user ID, PIN and the OTP to access the system. As e-commerce industry is growing rapidly, security issues become more crucial. Generally speaking, there are three types of identity authentication methods:

a. Identity authentication of something known, such as password.

b. Identity authentication of something used Object or Token, such as smart cards.

c. Identity authentication of some personal characteristics, such as fingerprint,

As of late, numerous remote confirmation systems utilizing smart cards and biometric-based client personality validation plans are proposed. For instance finger print access control systems are well known and mostly used technique [10]. Generally, biometric information is unique to each individual, this is the main advantages and differences of this systems.

Despite the fact that biometrics is viewed as the best and safe technique, one need consider the disadvantages. Every biometrics application technique has shortcomings which can bring about issues for its clients. Voice Recognition, Facial Recognition Detector, Iris Scanner & Recognition, Fingerprint reader, Veins and DNA Recognition each has specific problems. Biometrics system requires new and modern technology. Therefore, the cost for equipment is also expensive [11, 17, 18, 19].

Also, Lightweight Directory Access Protocol (LDAP) server password management system integration to the web server application is advised by many researchers. Such as, LDAP integration is used for managing many different integrated systems in companies, universities, e-commerce sites, soon such as university email service, lesson selection system, Wi-Fi networks [2, 14, 15].

In a few arrangements passwords are created by a token, an equipment token connected with the client, thus the password is not in view of the client's memory. Every time you need new token generated password. Some tokens generates password after the entering pin number. This step adds two-element verification method.

Every methodology has an alternate inconvenience or difficulty to use or need more time to adaptation process. In OTP based systems, the client must enter the new password with in fixed duration. If you failed during this period, user need to produce new one, User must follow all procedure again. This happens regularly and can be troublesome to the user. SMS based password has turned into a well-known remote verification in the world. Banking systems mostly prefers SMS as an additional step in login procedure [16].

3. Problem Definition

This organization where we implemented systems, are using a wide range of application, for example, email services, FTP services, news administration management programs, electronic program archive administration systems, video
editing design mechanization framework, advertisement management console and so forth. With this property a client sign in with a solitary ID and password to access an associated framework or in a few designs sign on at every framework independently. This is regularly refined utilizing the LDAP and put away LDAP databases on servers. These days LDAP validation is broadly connected to uniform personality confirmation framework in view of its cross-stage trademark and high accessibility [14, 15].

But some security policies force the users to change their password frequently. Sometimes user forgets their new passwords in any time after the setting new password. Because of that users cannot use their systems, when they forget it. This can be affect all chain of business systems in the organization. The users of the organization may be located all over the world, because of organization structure, should be allowed to change his/her password without any delay in secure way.

4. Implementation Details

The essential value of our system is in its simplicity and practicality for implementation and easy to adapt to other LDAP authenticated systems. Other advantages of our system are users can freely choose and change their passwords at anytime and anywhere. Apart from the other security login operation, this system doesn’t need any extra device and investment to set up. Furthermore, numerous researchers had attempted to adapt LDAP to their systems, but they didn’t focus on managing LDAP authentication. This system uses LDAP confirmation with the framework login and can manage LDAP password too [20, 21, 22].

Fig. 1. Project Architecture

This project is actualized web based asp.net C# programming language. The SQL server 2012 is used as the database (Fig. 1). We utilized the safe hash (SHA-1) encryption strategy for adjustment code checking and gateway served under the SHA 256 piece SSL (Secure Attachments Layer) confirmation. SSL gives a safe association between web programs and sites, permitting you to transmit private information on the web.

Fig. 2. Login screen (New Password Modul)

When user clicks the link on login page of the portal site, then user must fill information name, surname, User ID number, birth date, username and recorded GSM phone number. These information can be increased for extra information
such as ID serial number, birth place etc., is sent to the application from this site (Fig. 2).

The application fetches the necessary data of the user from the secure web services (Fig. 3). A Web Services is quickly rising and a popular standard in applications for sharing data over the web. Web service is a network accessible interface to application functionality, built using standard Internet technologies [12, 13]. That web service is supplied from Ministry of the Interior General Directorate of Civil Registration and Nationality. This service works as a service of cloud. The cloud computing service models is Software as a Service (SaaS) [22]. Recently many researchers are involved in cloud security, some of them advises MAC address matching [23], some of them advises intelligent systems to detect hackers activity [24] in cloud them automatically generate secure data.

![Application Flowchart](image)

As there exist concerns about storage and retrieval of data securely from cloud [25], the cloud based web service we use, is password protected and works only with dedicated special IP addresses of organization. These web services give various private information such as citizenship number, name, date of birth etc. about citizens.

During the password check step uses LDAP and uses citizen info web services. LDAP checks user phone number and username, citizen info web services is used to check user info’s. After the passing this step, system sends correction code SMS message to the user cell phone. These codes are encrypted by using the SHA-1 message. Before the applying SHA-1 method, we generate unique string for each user and then apply MD5 hash function before the applying SHA-1 hash function. For consistency of hashing policy with other applications in the organisation SHA-1 has been used. But to further decrease the vulnerability a more recent encryption method such as SHA-3 could be used (Table 1).

Table 1. Database Login History Table inputs

<table>
<thead>
<tr>
<th>ID</th>
<th>UserName</th>
<th>Operation</th>
<th>LoginTime</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>23251</td>
<td>test1234</td>
<td>08018CC.</td>
<td>23.03.2016.</td>
<td>172.30</td>
</tr>
<tr>
<td>23252</td>
<td>test1234</td>
<td>PasswordCh.</td>
<td>23.03.2016.</td>
<td>172.30</td>
</tr>
<tr>
<td>23253</td>
<td>test1234</td>
<td>AutoPassword.</td>
<td>23.03.2016.</td>
<td>172.30</td>
</tr>
</tbody>
</table>

Application checks user information from the web services, according to user’s additional information, it is not allowed to use user related info in the password; such as name, surname, birth year etc. This check prevents user related dictionary and guess based attempts. If the user tries to enter user related info, application shows warning message about that (Fig. 4). “It is not allowed to use Name, Surname or Birth Year in the Password!!! “
Password format for the new password will meet the following criteria: Password length – default length is 8 characters, but default may be overridden by specifying a password length on the Identity key Windows Logon policy, character set – the random password will consist of the following character set: a to z A to Z 0 to 9 printable symbols - !@#$%^&*()'"+_=\|/?<> Complexity requirements: The random password must not contain the User's User ID or parts of the User's full name that exceed two consecutive characters. The random password must contain characters from three of the four character set components listed above. Our password auto generator follows these basic rules (Fig. 5). If the user selects auto generated password, then the system sends the password by SMS to the user's pre-registered cell phone (Fig. 6). During this operation, if the user's entered a GSM number not equal to the pre-registered number, user is warned.

If company needs further strengthen the security of the authentication, it is easy to increase the complexity and length of password according new security policy.

The entire user related operations such as password change or phone number change operations, system sends automatic email for warning the users about this process.

5. Application Analysis

While the analysing the application use periods, we realized that most users had changed their password after the working hour from 18:00 PM to 09:00 AM (Fig. 7). User password change process has been done that each hour of the day. This is critical process for organisation, because of some departments are working for 24 hours a day.
The daily analysis also showed that; users are forgetting their password in a short period after changing password and Monday is the most password changed day of the week. The daily analysis also showed that a few users may need to change their password during the weekend, too (Fig 8). However, this may be a critical operation for continuity of work for certain organisations giving 7 day service.

Implemented application manages 7000 LDAP users’ passwords in the organisation. After the releasing the application, during the first 2 months period, 1598 user used the system. (Changed password or phone number) 1335 password change operation completed by users. In the 6 month period, the number of users increased to 3980 and in the next 2 month the number of users is increased to 4350 user (Table 2).

### Table 2. Password operation results

<table>
<thead>
<tr>
<th>Password Change Type</th>
<th>Count (first 2 month)</th>
<th>Count (in 6 Month)</th>
<th>Count (in 8 month)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Password Change</td>
<td>263</td>
<td>1176</td>
<td>1806</td>
</tr>
<tr>
<td>Mobile Password Change</td>
<td>12</td>
<td>70</td>
<td>119</td>
</tr>
<tr>
<td>Password</td>
<td>1062</td>
<td>2734</td>
<td>3355</td>
</tr>
</tbody>
</table>

Day use of the system has been shown to increase the rate day by day. Due to the holiday period more users forget the password, the system's operability rate was greater during this period. (July - 986 and August - 1020)

### Table 3. Systems Comparison

<table>
<thead>
<tr>
<th>Properties</th>
<th>Our System</th>
<th>Other LDAP systems</th>
<th>Biometric Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Integration</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SMS</td>
<td>yes</td>
<td>some</td>
<td>no</td>
</tr>
<tr>
<td>Trusted user related info Password Check</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Strong Correction/Challenge</td>
<td>yes</td>
<td>some</td>
<td>yes</td>
</tr>
</tbody>
</table>
6. Conclusion

In this paper, we have proposed another password verification system less vulnerable to brute force attacks associated with LDAP combination. This methodology proposes a compelling confirmation framework which robustly and effectively set new LDAP passwords with sending over GSM system. Particularly issue of strong client password is achieved, which is normally weak in most other applications. This framework warns clients about the shortcoming of password and not permits to utilize predictable client related password. This method also decreased IT costs because of lower number of IT help center calls about password change request.

This framework can be utilized for validation login data of all online applications utilized as a part of the organisation. It can be adjusted to be used with different security frameworks’ login modules, as well.

References


