Versatile Approach For Creating, Managing And Strengthening Lost Free Password Using Iterative Alignment Algorithm

Chandra Sekhar Kolli, Suma Mallidi, Sai Kiran M, Chandra Kishore D

Abstract : Even after with years of research and availability of many sophisticated authentication methods available, Authentication with passwords are still dominate latest approaches. The main aim of this article is to develop a new algorithm to strengthen password-based authentication approach. Existing methods has a very poor security practices as a result server can be very easily compromised. We have designed and developed a new versatile approach to create, manage and strengthening lost free password algorithm using Iterative Alignment Algorithm.

Index Terms: Cryptographic, hash-based algorithm, security, management, password, multiple, complexity, security

1 INTRODUCTION

In our daily life we use different websites like Gmail, Facebook, internet banking, e-commerce sites, educational sites etc. [1]. Each one of these records are validated by utilizing a user name and a secret password. We for the most part utilize a solitary solid secret password for each one of the several sites [9]. We generally use a single strong password for all the hundreds of websites. But using a single password or multiple passwords is how much safe and secure [12]. Not just for sites we additionally utilized passwords for checking of PCs framework [1]. This major key word turns as a first line of armor against the unauthorized or unpermitted access [1].

Single Password vs Multiple Passwords

Single Password

When we use single password for multiple websites or systems. Then it's easy for the third party to access all accounts when he knows one [1].

Multiple Password

When we use multiple passwords, it is difficult for third party to access the other when he knows one password. But here there is a problem of forgotten of passwords [1].

Security threats of password

Mainly we have four security threat attacks on passwords

1.1 Over shoulder Incursion

When a computer user enters his or her password, if another person had a glance on what was entered and hence that authorized attacker steals the password that was typed by observing over the shoulder or using an electronic device like cameras or other picture capturing devices [12].

- *Chandra Sekhar Kolli is currently working as Assistant Professor in Computer Science and Engineering department in Koneru Lakshmaiah Education Foundation, Vaddeswaram,Guntur District, 522 502,India. E-Mail: usercsk@gmail.com*
- *Mallidi Suma,Sai Kiran M,Chandra Kishore D is currently pursuing Bachelors degree in Computer Science and Engineering in Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, 522502, India*

1.2 Brute Force Incursion

As we all that the maximum length of a password is finite and that to eight alphanumeric characters, a hacker might be able to create a different codes or computer instructions that naturally generate generate our keywords by using these generated he or she try all possible combinations they finally crack our passwords. If they were not able to found the password in one iteration, they continuously iterate this attack. Brute Force attack is a recursive technique [12].

1.3 Sniffing Incursion

While a keyword is sent in a network it can also be apprehend by using some sniffing tools like FeaKey logger. All the information about the user name and password is stored in that sniffing tools. Then the third party can easily know and access [12].Here there is an example of Feakey logger which comes under sniffing toolsIt is an extension to our google chrome simply we can download it and add it to extensions of our browser i.e., How Fea Key Logger is downloaded and added as an extension to the google chrome was shown in Fig. 1. and Fig. 2. When you sign into Gmail as shown in Fig. 3. The password will be stored in fea Key Logger as shown in Fig. 4.

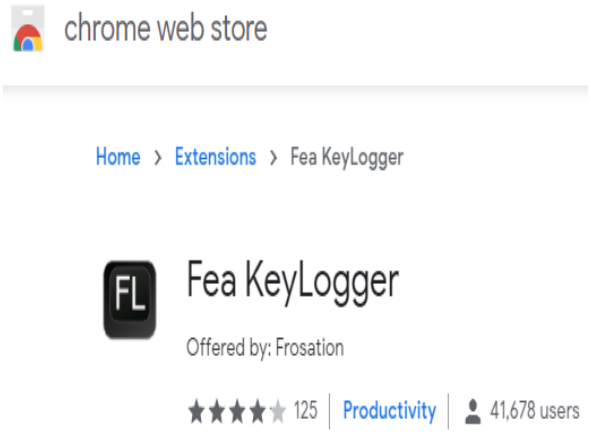


Fig. 1. *Fea key Logger*

***Fig. 2**. Add to chrome Button*

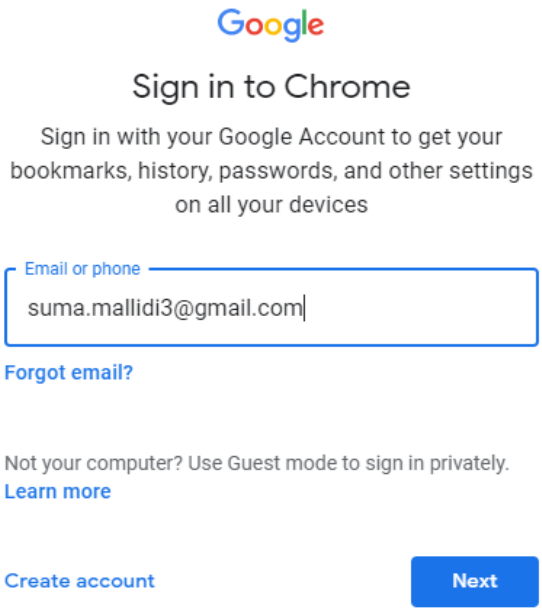


***Fig. 3**. Gmail sign in*

***Fig. 4**. Passwords in Feakey Logger*

1.4 Spoofing Incursion

It is an interesting attack that in this a hacker or an attacker creates an illusion login screed which is very much identical to the original login screen. As user don't know this trick and if he tackle into this his user key will be recorded in his particular database or even directly sent to the attacker or hacker [12].

Different methods that are used to secure our passwords

1.5 Single Sign

In this technique the users can only identify themselves only once in that authentication server by using their own password. Here we can use a single password for a multiple site. But all these are only single sign on [12]. But the encoding in the backward of the server should be stronger in order to take different passwords at different login times [12].

1.6 Password Token

In this technique mainly there are two main authentication keys one is token and other one is token. Here the user need not to memorize a password. Based upon the token and pin a password is generated by it every time when we are trying to login. Here a token is required for the authentication of the user. It leads to additional cost [12]. If the user forgot to bring the token then he is not able to access the system. Here the token is securely maintained all the time [12].

1.7 Hashed Technique

It is a server-side encryption (encoding). Here the plain data is stored in the server later it undergoes into hash-based function. We use private key here in hash function. It provides a server-side encryption so whenever it is hacked the hashed passwords are hacked but not the original plain passwords. As private key is computed individually by each of the sides i.e., both sender side and receiver side by using a common methodology [12]. But is a time taking procedure and it requires a large number of computations to be performed in order to restore our forgotten password but it provides a large security as it is very difficult to hack by an attacker [12].

1.8 Salted Technique

Here the plain passwords are concatenated with the key word called salt. We can concatenate it to our required length [12]. Here in this also the hacker doesn't know the original passwords whenever it is hacked [12]. Not only with salt we can concatenate with any other key word up to our own length [12]. But this method does not produce much security because when the user able to know one password for one particular website then it is very easy for him to know the different passwords for different websites because a common key word is used [12].

1.9 Public Key Infrastructure

Public key infrastructure is also called as PKI. It is a technique which uses mathematical algorithms. Through this we can provide data integrity, data confidentiality and authentication. It uses digital certificates for the proof at the time of data authentication [12]. It is a kind of digital document. It uses a kind of key called public key for witness [12]. This certificate is created by a trusted certificate authority popularly known as CA [12]. later it signs on the digital certificate by using certificate authority (CA'S) private key [12]. Thus, an authentication is done by using digital certificates

Security issues in using digital certificates:
As private is not known to even second party it must be kept is a secret and secure place. Certificate authority must be trusted and it need to more secure and unique its validity must be maintained in digital certificates. It must be invalid when it exceeds the validity time.

2. LITERATURE REVIEW

J. Alex Halderman and Edward W. Felton [1] have used a technique called "key-stretching" it was a repeated application like a hash-based technique. It was a regular hash function-f (), is replaced with a new function-$f^k()$, where $f^k()$ is computed by repeatedly applying the hash function k times.in this technique they also increased the time which as required to find the hash function. Danuvasin Charoen [3] reviewed about the human memorability regarding passwords and divided the memory into three stages. According to him the first stage of memory can be termed as the when the acquisition process occurs as the first step. Second phase is the user memorizing the password and the last phase was the user recalling the password.by using this paper we were able to decide among the single passwords against the multiple passwords and also, we decided about the length of the digits or characters in the final password. Shirley Gaw and Edward W. Felton's [4] work concentrated on increasing the password management strategies. Their different method allowed us to measure results with the number of logins attempts rather than relying on the users to recall password reuse. Ian Jermyn's [5] work on graphical password schemes have achieved better results than conventional textual passwords and their approach was using the graphical devices for inputs. Scott Standridge [8] have reviewed about the best password management practices. He also added that we can know about the strength of our password using password strength report so that we can alter our password depending upon the report.

3. ANALYSIS

Below mentioned were some of the examples of the wrongly chosen keys for authentication [4]. These are easily cracked or hacked by the hackers. Sometimes it is very difficult to develop a mechanism or different websites until or unless we use a centralised database.
In order to use this password with more safety and security all users must aware of some basic's tricks and tips [12].
"passwords" –it is the most easily guessed password. hacker's initial password [12].
"administrators" –it is a login name [12].
"cisco" - a famous name [12].
"suma" – it is a name [12].
"bbbbbbb" – repetition of same letter.
"abcdefghi"–a collection of consecutive letters.
"acegik"-Not a collection of consecutive numbers but it follows a particular sequence which very easy to guess [12].
"123456789" –It is also a collection of consecutive numbers.
"qwertyuiop" - adjacent keys on the keyboard in addition it is the first row in the alphabetical part of the keyboard [12].
"computer" - a well-known word for password users [12].
"computer123" –a little bit and simple variation in the well-known dictionary word [12].
"COnnectIon" –a slight variation with C as c, O as o and I as i [12].
"ddddddddd"-repeating the same alphabet [12].
"dcba"-reverse of a consecutive alphabetical series
"987654321"-reverse of a consecutive number of series [12].
"a1b2c3d4"-a combination of consecutive alphabets and numerical. It is little bit difficult to identify when compared with the above passwords [12].
"username"-it is available in the page itself [12].
"Facebook"-Most popular website name [12].
"sender"-A well-known terminology used in this this mechanism [12].
"receiver"-An immediate brute force word after sender.
Do not use user name in password creation directly
Do not set your family member's names.
Do not set your personal information like card names like Aadhar card, pawn card etc. while creating a password.
Do not set your passwords with only digits or alphabets or special characters. Use them in a combination.
Do not set a combination or a guessing patterns like alternate letters, Consecutive letters [12].
Do not use keys on the keyboard like "qwertyuiop".
Do not directly use a direct word in English or French [12].
Do not set a reverse word as a key.
Do not set known abbreviations like ISRO, NASA IPS, IAS, CSE, DSP etc. [12].
Do not follow a technique of password reusing.
Do not set a single password for all accounts. Its suggested to maintain one type of password for important accounts and other type of passwords for un important accounts [12].
Do not note your own passwords in any place which is very near to the computer or also in different parts of computer like keyboard, mouse etc.
Do not reveal your password to anyone under any circumstances [12].
Do not send your unencrypted password in any social media websites.
Always avoid clicking ok on remembering your password because your system may be in some other person use [12].
Do not publicly read the file or open the file which contain the password.
The following are the dos of password management
Use a mixed password it may contains alphabets, numerical or even special characters.
Use a password which is very easy to remember at the same which is very difficult to hack by the third party.
Use a password which is very easy to type on the keyboard and also make sure that you are typing your password without looking the keyboard it prevents hacking the password through secretly observing the password.
Frequently change your password at least in a duration of 30 days.
Always change the initial password or first password immediately at that login time.
Change your password when you believe that your password is known or hacked by someone.
Select different passwords for different accounts.
Upon receiving the new passwords immediate change, the initial password.
Change all the system default passwords as soon as possible.

4. METHODOLOGY

In order to make our passwords more secure and safe. One advanced methodology is [1]

Construction

First step is to construct a variable. Let us say it as V i.e.,

V=user name + Master Password.

Second step is to construct another variable. Let us say it as U.

U=V + site name+ Master password.

Now U becomes the final password.

Example:

If a person wants to create a secret key for Gmail site

Therefore, site name is gmail.

V=user name + Master Password.

V=chandramallidi+malli456789

V=chandramallidimalli456789

chandramallidi and malli456789 username and master password.

U=V + site name+ Master password.

U=chandramallidimalli456789+

gmail +malli456789

U=chandramallidimalli456789

gmailmalli456789

U is the final secret key.

Security Issues for the above proposed theory

After completion of the above two steps our password becomes very difficult to hack because it is not a single password which is common for all other websites [1]. Even it is not repeated and very easy to guess. Here the methodology which we use is difficult to identify. And its space complexity is much greater [1]. In addition, we have four other issues like

4.1 No Information

In this technique the hacker has no information about the user or about the password [1]. It was a repeated technique which follows a methodology called velocity control attack [1]. It was in a high risk when the attacker does not succeed. If the attack made by an attacker is successful the attacker only gets a site-specific password, which is not sufficient to attack another website password [1]. Even if he/she hack the password she only left with that site-specific password not with all passwords of that particular user because the user is maintaining different passwords for different websites.

4.2 Stolen Site

In this attack the user attacks the password by convincing the user to login into a similar website which appears like the original [1].

4.3 Stole Cache

In this type of attack the attacker or the hacker compromises the user and steals the computer [1].

4.4 Stole Site and Cache

In this technique the user tries to get the final passwords by using all the intermediate passwords like master passwords, tokens etc it was a brute force technique [1].

Drawbacks of above methodology

Length of the password generated was much higher which leads to a problem called password forgotten. Even though it has a fixed methodology it is very to difficult to calculate the password each and every time. It takes a lot of time while operating that particular website by typing that much large password.

Solution for the above methodology

In modified methodology We have

Step 1.

Calculate value of variable V i.e.,

V=user name + Master Password.

Step 2.

Select one operation to apply on variable V.

A. Even Place Deletion.
B. Odd Place Deletion.
C. Prime Place Deletion.
D. Even Place substitution.
E. Odd Place substitution
F. Prime Place substitution.

Even, Odd and Prime Place Deletion operations are iterative techniques. And its iterative condition is.

```
do
{
Perform Selected Operation;
}while(V>=sitenamelen);
```

For Even, Odd and Prime Place Deletion operations we follow substitution methodology. It follows.

Character1 =character + sitenamelen;

character1 is between (A to Z) or (a to z).

Step 3.

Calculate value of variable U i.e.,

U=V + site name+ Master password.

Repeat step 2 substitute variable(U) in place of variable(V).

U is final secret key.

Example

First Variable (V) is

V=user name + Master Password.

V= chandramallidi+malli456789

V=chandramallidimalli456789

chandramallidi and malli456789 username and master password.

If selected operation is A i.e., Even Place Deletion

Iteration 1

V=hnrmlia1468

Here length of V>Site Name length

So according to our methodology we iterative this until V<Site Name.

Iteration 2

V=nmia48

V>Site name length

Iteration 3

V=ma8

V<Site name length.

Therefore, first variable V is finalized.

Second Variable (U) is.

U=V + site name+ Master password.

U=ma8+gmail+malli456789

U=ma8gmailmalli456789

If selected operation is B i.e., Odd Place Deletion

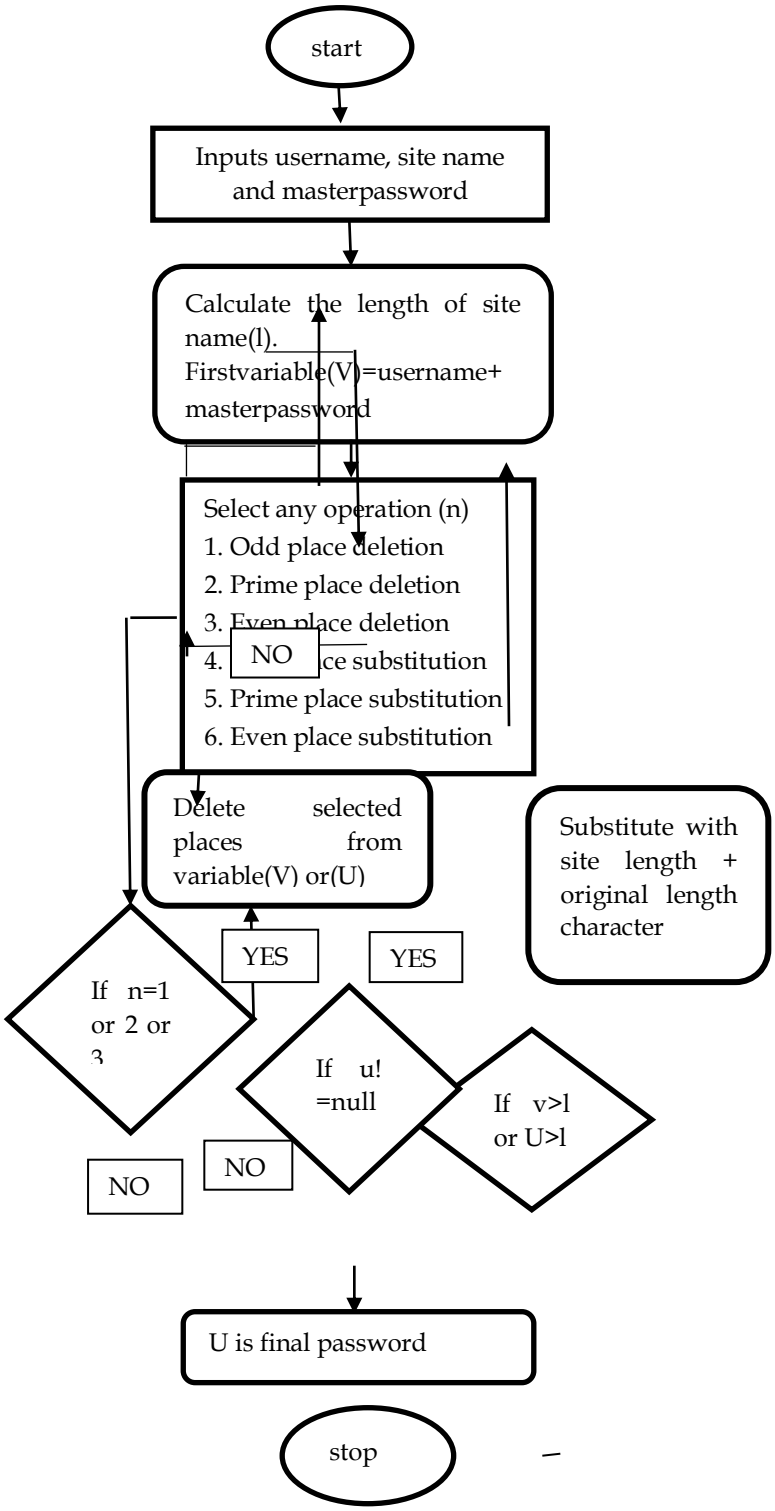
Iteration 1

U=agalal468

Here length of U>Site Name length

So according to our methodology we iterative this until U<Site Name.
Iteration 2
U=gll6
U<Site name length.
Therefore, our second variable u is finalized.
Here second variable is our final password.

5.FLOW CHART



6. USES

Here by using the above methodology we can manage our password with more safe and secure. Here the length of our main password is also small after applying the above solution [6]. We can easily access our website by typing a minimum length main password. As its methodology is very clear and simple to implement even if we forget the password then becomes easy to compute the original password easily without any access of forget password option provided in that particular website [7]. It is much difficult for hackers to hack the password if he knows one password for that particular website. Here we use same methodology in calculation of password but not the same password for different websites [11].

7. CONCLUSION

Passwords are the most frequently used keys for authentication of users. Attackers consistently tries to break the frame work that was implemented in password generation. We have developed a versatile algorithm to create, manage and strengthening lost free passwords using Iterative Alignment Algorithm. With the help of this new algorithm any user can authenticate themselves in front of an authentication server with his Strengthen personal key. We can also use different access control systems to generate personal passwords and it was possible to decrease time and space complexities.

8. REFERENCES

[1] J. Alex Halderman, Edward W. Felten, Brent Waters. A Convenient Method for Securely Managing Passwords. Princeton University, pages 3-4, 2004.
[2] Y. Alan, J. Jeff, B. Ross, and A. Alasdair. The memorability and security of passwords – some empirical results, pages 13-14, 2000.
[3] Danuvasin Charoen, Password Security, NIDA Business School, National Institute of Development Administration, pages 2-3, 2014.
[4] Shirley Gaw, Edward W.Felten, Department of Computer Science Princeton University Princeton, ,Password Management Strategies for Online Accounts,pages 5-9,2006.
[5] Ian Jermyn, Fabian Monrose, Michael K. Reiter, Alain Mayer and Aviel D. Rubin. The design and analysis of graphical passwords, pages 4-6 ,1999.
[6] Alain Mayer, Ian Jermyn, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. The design and analysis of graphical passwords. pages 5-10, 1999.
[7] Yehuda Lindell and Rosario Gennaro. A framework for password-based authenticated key exchange. In EUROCRYPT, pages 3-16, 2003.
[8] Scott Standridge, Advisor: Rob Vanden brink. Password Management Applications and Practices pages 2-3, 2016.
[9] David Silver1, Suman Jana1, Eric Chen2, Collin Jackson2, and Dan Boneh1.Password managers Attacks and defences by 1. Stanford University 2. Carnegie Mellon University, pages 3-17, 1998.
[10] Alain J. Yossi Matias and Eran Gabber, Phillip B. Gibbons, Mayer. How to make personalized web browsing simple, secure, and anonymous. In Financial Cryptography, pages 17–32, 1997.

[11] P. Youn and M. Blanchou. Password managers: Exposing passwords everywhere, pages 2-4, 2013.
[12] The government of the Hong Kong special administrative region. Password Management, pages 5-16, 2009.