ISSN No. 0976-5697

Volume 6, No. 1, Jan-Feb 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Secured Session Password Protection System Using 3DPA Methodology

Prof. Anil Hingmire
Department Of Computer Engineering
Vidyavardhini's College Of Engineering And Technology
Vasai Road, India

Mr. Himanshu Musale
Department Of Computer Engineering
Vidyavardhini's College Of Engineering And Technology
Vasai Road, Maharashtra, India

Mr. Kalpesh Gosavi
Department Of Computer Engineering
Vidyavardhini's College Of Engineering And Technology
Vasai Road, Maharashtra, India

Ms. Priyanka Notani
Department Of Computer Engineering
Vidyavardhini's College Of Engineering And Technology
Vasai Road, Maharashtra, India

***Abstract*—** In this paper, we are proposed a new methodology for password protection named 3DPA. Mostly textual passwords are used to secure data or user accounts. However these can be cracked by the application of various brute-force attacks as the maximum password length is fixed and there are a finite number of possibilities which exist. Also textual passwords are vulnerable to eavesdropping, dictionary attacks, social engineering and shoulder surfing. The proposed system generates session passwords using a 3 dimension pairing authentication technique which are resistant to shoulder surfing. The system uses cryptography to preserve confidentiality goal.

Keywords:brutforce attack;eavesdropping;social engineering attack; shoulder surfing attack; crptography; confidentiality etc.

I. INTRODUCTION

Recently there has been a great emphasis to provide more security for passwords. The 21st century is the more advancing age of internet and related contents, highly exposing data which innovated before a minute or say as to some seconds. The most traditional method for authentication is textual Password. User's first choice for authentication is textual passwords. Mostly users choose short and simple password so that they can be easily memorized and can be recalled at the login-time. In common it has been surveyed that an average users has to memorize at least 3 passwords. Again in addition to this the user has to remember password for banking, e-commerce, and social networking sites and also email accounts. Short and simple textual passwords are easy to remember, but can be easily hacked while random and lengthy passwords are secured but hard to remember. To overcome this problem graphical authentication schemes were proposed. But this scheme had many problems like they were easily prone to shoulder surfing attacks. Many others authentication schemes were proposed to overcome the shoulder surfing attacks but they had many drawbacks like they take more time to login, usability. In this paper there is an authentication scheme that is designed to provide more security than that of textual for a session. Session passwords are used only once.

Everytime the users enters a session he has to enter another password. Once the session is over that password becomes of redundant for next session and the current session gets terminated. Session passwords are more secure as everytime the session start a new password is created and they are not prone to dictionary attacks, brute force attacks and shoulder surfing attacks [1].

II. WEAKNESSES OF EXISTING PASSWORD SCHEMES

A. *Attack On Ebay Website.*

Don Reisinger, in his article named "eBay has been hacked, requests all users change passwords"[2], said that the site's system might have hacked and along with a database having users account details seemed to be affected. While company denied that the reports are falsely interpreted, the company has suggested it's customers to change their secret information. They found out that they might have been a target of a cyber attack. These results the shares of eBay had down by 2 percent after the news of hack.

That database of eBay was affected which includes customer's personal information but the company had confirmed that their customer's financial information is safe.

B. *4.93 Million Gmail Passwords Leaked By Hackers.*

Ravi Sharma has written in his article known "4.93 million Gmail passwords leaked by hackers"[3], Google accounts has been hacked by Russian hackers which affects approximately 4.93 million users includes their secret credentials. But the biggest problem arises as the same Google account password is used like Gmail, Maps, YouTube, Plus and Drive etc.
The account details were available on a website btcsec.com which is a bitcoin forum and they were posted by a user named Tvskit. On site the user has mentioned that almost 60 percent of secret credentials are still active by users. However in a blog post Google refused the claim and said only few secret credentials are active and its automated anti-

hacking system might have blocked many login attempts done by the attacker.

C. *Hackers have managed to break into 7 of the top 15 banks.*

Jose Pagliery has written in his article known as "Hackers have managed to break into 7 of the top 15 banks"[4] that World's biggest financial bank's like JPMorgan Chase (JPM) has been hacked. The hackers have invented a new malware technique which break the computer system and is able to view or delete or manipulate bank records. Attackers had entered very closely into the system and internal records of bank were accessed which means they can steal information of their customers. These sacrifices customers security and confidentiality. Banks future investment strategies are also at stake. The chief cyber security officer of Trend Micro Mr. Tom Kellermann has suggested that attackers may destroy banks' entire network system.

D. *7 Million Dropbox Passwords Hacked.*

Steve Kovach has revealed in his article "Nearly 7 Million Dropbox Passwords Have Been Hacked"[5] that Nearly 7 million Dropbox usernames and passwords have been hacked, as users allow third party applications from their account to access Dropbox. The attackers have hacked nearly 6.9 million secret credentials which belong to Dropbox. The biggest problem here signifies that almost 90 percent users allow third party applications by well known services to use their platforms. Dropboxs' personal servers were apparently not attacked. Still the services allow third party access, which became a target for attackers to get personal information from the Drobox users.

III. NEW PROPOSED SYSTEM

In this paper we are proposing a new authentication technique which is more robust, secure and reliable. The name of this technique is 3D Pairing Authentication technique. It consists of 2 phases as given below:

Phase 1: Registration Phase

Figure 1: Example of Registration Window

During the registration phase the user enters his/her username and password. And following steps are performed during the registration process:

- **Step 1**: We take the User ID & textual password from the user.
- **Step 2**: Calculate the length of the password (L).
- **Step 3**: Add the jumbling characters to the password which should be same in number as L at the specific positions. Save this as JP.
- **Step 4**: Right shift the characters of JP by L. Save this as EP.
- **Step 5**: The EP now is stored at SERVER Database.

Phase 2: Login Phase

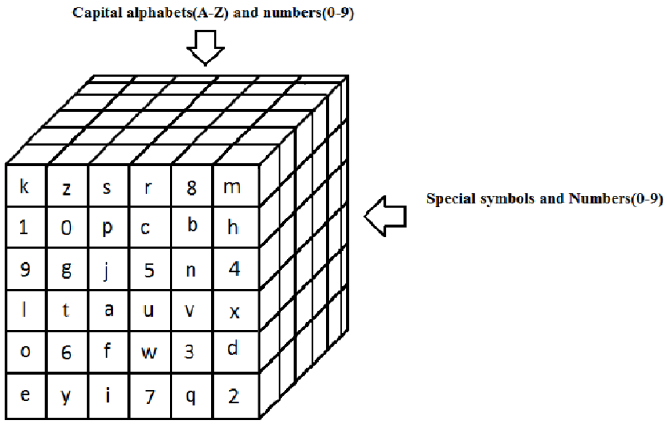


Figure 2 : Example of 3-D Cube

During the login phase a 3D Cube is seen by the user along with two text boxes to enter his/her username and password. First of all the username of the user is tested and only if the user name is true user can move forward for validation of password. For the selection of password user has to make use of 3D Cube of size 6*6*6. At a time a user can see only 3 faces of the 3D Cube and each face has 36 grids in it. The 3 faces of the 3D Cube that are visible to the user have contents such as capital alphabets(A-Z) and numbers(0-9) on first face, small alphabets(a-z) and numbers(0-9) on second face and special symbols and numbers(0-9) on third face. Now from the cube show in above figure the user has to select his/her password's letters, digits and special symbol (if present). Pairing authentication technique is used in 3D Cube as shown below:

-

- ***Case 1: If the length of the password is even***

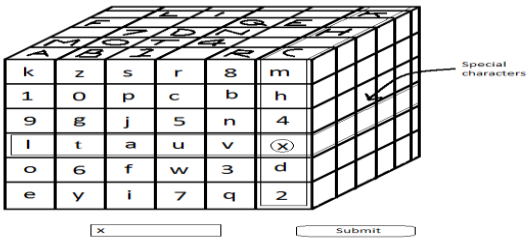


Figure 3: Example of 3-D Cube Login

In the figure shown above if the password is 'kalpesh9' i.e. it has even length than pairing of two initial letters is as done in the figure and the first character of session password generated will be 'x' in similar manner for the whole password 'kalpesh9' of length 8 we get a session password of

length 4 i.e the length of session password becomes half of the original password length.

- **Case 2: If the length of the password is odd.**

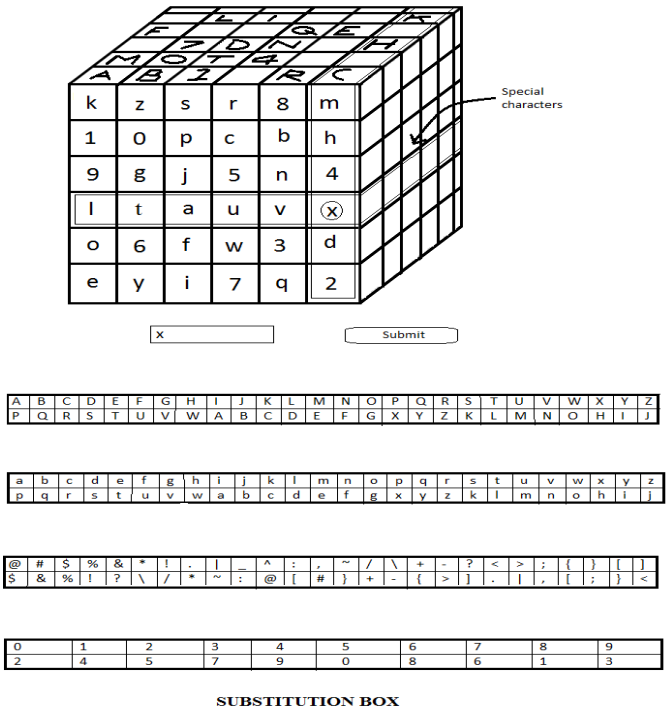


Figure 3: Example of 3-D Cube Login with Substitution Box

In this case along with 3D Cube we have a substitution block so that the last remaining character of the password which cannot be paired can be substituted with the help of substitution block shown below. Let's take an example, if password is 'kalpesh' which is a odd length password than the paring for first two initial characters of the password is done is similar manner as in case 1 and we get the first character of session password as 'x' but for the last character of the password in this case i.e 'h' we use substitution box and substitute it with 'w'for generation of session password.

IV. ALGORITHM AND FLOWCHART

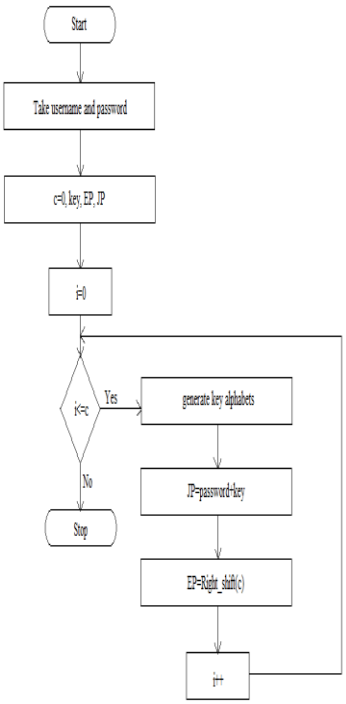
A. *Registration Phase*

1. Start user_reg_password (username, password)
2. Input username
3. Input password
4. var c=0, key, EP, JP //EP-Encrypted Password
   //JP-Jumbled Password
5. c=count(password) //calculates length of the password & character count
6. For i:=0 to c
   Key[i]=random_alpha() //generates random key alphabets
   end
7. JP=password+key //jumbling the password with random key alphabets
8. EP=Right_shift(c) //do right shift with key c
9. Send EP
10. Stop

Password Extraction at Server side

1. Accept EP from client
2. Store EP to database

3. FLOWCHART



B. *Login Phase*

1. Start user_login_password (username, password)
2. Input username
3. Input password
4. Var c=0, DP, JP , l=0 //DP-Decrypted Password,
   JP-Jumbled Password
5. Boolean temp=false
6. If(username==db(username)) //db(username)-Usernames stored in Database
   Temp=true
7. If(temp==true)

Extract db(EP)

8. c=count(EP)
9. key=c/2
10. JP=left_shift(key)
11. DP=JP-key
12. l=count(DP)
13. If l%2==0

Compute session password using pairing authentication technique from randomly generated cube

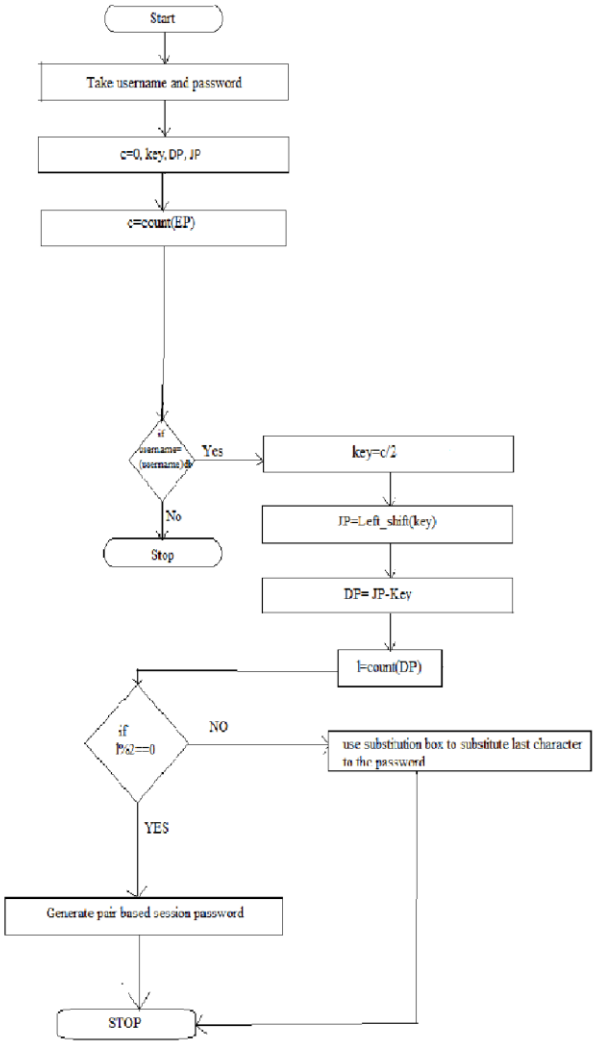
Else

- Compute session password from randomly generated cube for maximum number of pairs that can be generated
- Use substitution for remaining password character

14. If(DP==password)

User is authenticated

FLOWCHART:



V. CONCLUSION

In this paper, a authentication techniques based 3D Cube and pair-based scheme is proposed. These techniques generate session passwords and are resistant to dictionary attack, shoulder-surfing and brute force attack. This techniques use grid for session passwords generation. However this scheme is completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness. Also the proposed authentication scheme can be used in a variety of applications that demand more security and reliability.

VI. REFERENCES

[1] Jay Patel, Sagar Padol, Bhushan Kankariya, Kainjan Kotecha, "Authentication for Session Password using Colour and Images", International Conference on Recent Trends in engineering & Technology in International Journal of Computer Applications(0975 – 8887), 2013.

[2] Don Reisinger, "eBay hacked, requests all users change passwords",http://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/

[3] Ravi Sharma, "4.93 million Gmail passwords leaked by hackers",http://timesofindia.indiatimes.com/tech/tech-news/4-93-million-Gmail-passwords-leaked-by-hackers/articleshow/42241159.cms

[4] Jose Pagliery, "Hackers have managed to break into 7 of the top 15 banks", http://money.cnn.com/2014/ 08/ 28/ technology/security/bank-hack/index.html? sr=tw082914 bankhack1030aVODtopPhoto

[5] Steve Kovach, "Nearly 7 Million Dropbox Passwords Have Been Hacked", http://www.businessinsider.in/Nearly-7-Million-Dropbox-Passwords-Have-Been-Hacked/articleshow/44809315.cms