http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (6): 1161-1169, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1161.1169

Effective Methods for Secure Authentication in Vulnerable Workflows using n×n Passwords

S. Safdar, M.F. Hassan, M.A. Qureshi and R. Akbar
Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Malaysia

Abstract: The main objective of the research is to propose the effective methods of using two-dimensional n×n passwords in terms of providing secure authentication to inactive users of the system during vulnerable state. The proposition is based on the fact that if the system goes in to unsafe state due to some intrusion threat then to make the system available to the end user, it is required by the users to re-authenticate using special mechanism. These users can become active once authenticated and can continue their tasks using alternate services. These n×n passwords are long and complex, hence are difficult to memorize. But these can be very useful in certain alarming situations such as in case of system being under threat. Proposed methods provide the maximum benefits in terms of secure authentication to the system resources that is under threat. Three methods have been proposed that are classified on the way the password is created or generated. The strength and limitations of all the proposed methods has also been analyzed.

Key words: n×n password, bit entropy, server generated passwords, user created passwords, hybrid passwords, rotational reformation

INTRODUCTION

Passwords have been widely used for authentication purposes in the computer systems. Various attempts have been made to make the passwords more strong and difficult to guess. For this purpose, the long passwords have been recommended but were not so much complex. Hence including alphanumeric characters in a password increases the strength furthermore (Smith, 2002). Then password strength was further enhanced using all keyboard characters. But as we try to strengthen the password, simultaneously the large and complex passwords are discouraged by the users because these are difficult to remember (Smith, 2002; Helkala and Snekkenes, 2009; Florencio and Harley, 2007; Gaw and Felten, 2006). Hence, the medium strength passwords are in common use by most of the users and systems are made in such a way to provide additional measures for the security. But does this mean that we ignore the tremendous strength of long passwords? The answer is absolutely not. The efforts should be made to take advantage from the long and complex passwords to strengthen the system in an effective, efficient and more useful ways (Safdar and Hassan, 2010). Those methods should be adopted that can assure much tighter security as well as effective management of long passwords so that memorizing the long passwords would not be the problem for the end user.

Two dimensional n×n passwords are the new passwords that are defined in x-y plane. These passwords are very strong as these are long and complex in nature. The main issue associated with those passwords is their better management for their effective usage. Despite of complex one can acquire maximum benefit from those passwords in terms of great strength if these have been effectively utilized only under alarming situations. Such situations may occur whenever some special measures are required for data security and integrity. In this study the usage of these n×n passwords have been discussed when the system is under threat and is required to be available to its user even in vulnerable state using an alternate path of execution (Safdar *et al*., 2009, 2010a).

When IDS (Intrusion Detection System) indentifies an intrusion attack on the system, usually a system goes in to wait state and becomes offline temporarily until the system is recovered and in the safe state again. The ongoing transactions in this case become rollback and redone once the system becomes available again. One of the frameworks suggests keeping the system available even in the unsafe state by providing an alternate path of execution (Safdar *et al*., 2010b). But in this case the special authentication needs to be done using an unconventional way, such as two dimensional passwords (Safdar and Hassan, 2010; Safdar *et al*., 2010a). Figure 1 shows the overall view of the framework for alternate execution path in vulnerable systems. It may be noticed

Corresponding Author: S. Safdar, Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Malaysia

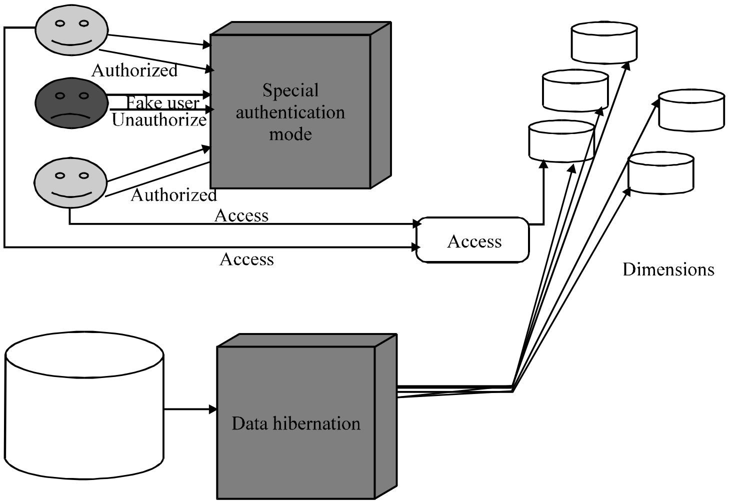

Fig. 1: Framework for alternate execution of workflows under threat

that a special authentication module requires special mechanism to make the user login much more securely in an environment where the probability of being hacked is much high. It is recommended to use two-dimensional passwords effectively and securely managing the authentication in case of the threat scenarios of the system to make it available to the end user. Data hibernation shifts the data to the designated dimensions for the provision of services alternatively.

This study deals with the methods of adopting the two dimensional passwords in all possible aspects to achieve two goals. One is to provide remarkable security to the user utilizing complete advantage of long and strong passwords where as the second would be an effective management of these long passwords so that the end user might not find it difficult to use. For the sake of simplicity, the two dimensional passwords of n×n nature have been considered in this study. The coming sections include the background study as well as the pros and cons associated with two-dimensional passwords. Then the method of calculating the strength of the password by calculating its entropy will be discussed. Then study also includes rules of formalizing the passwords. The proposed methods of using these n×n passwords have been discussed followed by the analysis of proposed methods to consider the best methods. Conclusion and future directions have been discussed afterwards. These passwords are not meant to be used all the time, hence these are used occasionally. One of the main areas of applying those passwords is providing the users an authorized access to the system resources when the system is in vulnerable state but is made alternatively available.

Password is a basic and very famous mechanism that had been used from a very long time for ensuring security of computer resources. Making passwords strong has always been a focus of the study. The trend of using the long passwords, using alphanumeric passwords and using passwords that include special characters are the major and important moves for making the passwords more strong. But as the passwords are becoming lengthy and complex, the problem arises of memorizing them. People tend to make easy to remember dictionary words passwords that can be hacked easily and are insecure (Helkala and Snekkenes, 2009; Florencio and Harley, 2007; Gaw and Felten, 2006). Hence various mechanisms have been used to manage passwords in such a way that it becomes stronger and can easily be memorized. A very famous standard is provided by the NIST (Burr *et al*., 2006; Red Kestral Consulting, 2004; Allan, 2004) that properly manages the passwords in such a way that they become easy to memorize and can equally be difficult to break. In all of the particular efforts, the long and difficult passwords are always discouraged but the fact cannot be avoided that the long and complex passwords are the strong one that can provide maximum security and hard to break. There are mechanisms to protect the data transmission using digital authentication certificates (IBM ISeries, 2009). These certificates use the public key and private key infrastructure (Tan *et al*., 2009; IBM ISeries 2009) to provide the encryption services to the data transmission to retain data integrity. But if the passwords are hacked and break then these certificates might also be accessed by unauthorized user and can be misused. Hence, making password strong and unable to break is of the prime and important goal for the system security. For this purpose, multiple modes of passwords have also been in common use as by the SQL Server database (Hsueh, 2008) that uses windows authentication mode as well as database authentication mode. But still there is a need to providing passwords with much more strength to make systems work even under a vulnerable state. Hardware based biometric passwords are also been implemented but are expensive (Yang and Yang, 2009; Li *et al*., 2009). Graphical passwords that may hide in images are also been the field on which currently study is going on (Oorschot and Thorpe, 2008; Wiedenbeck *et al*., 2005). The concept of two dimensional passwords has also been explored that are much stronger and not expensive as well (Safdar and Hassan, 2010; Safdar *et al*., 2010a). Work has to be done to explore the significance of multidimensional passwords as these are very hard to memorize and manage. Hence this paper will be based on the fact that long and complex passwords are the strong one and will cover the significance of using two dimensional passwords effectively under the intrusion threat circumstances (Safdar and Hassan, 2010). The problem of memorizing those passwords can be solved by effectively managing those passwords which is the prime goal of this study.

PROS AND CONS OF USING TWO DIMENSIONAL PASSWORDS

The users mostly discourage long and complex passwords, as they are hard to memorize. User always try to pick that password which is easy to recall, the password might be some statement that the user uses frequently or might be some word that is more commonly associated to his/her life. Due to this practice the user tends to change the system generated passwords to the one of their own and those passwords may not be as strong (Helkala and Snekkenes, 2009; Florencio and Harley, 2007; Gaw and Felten, 2006). If we consider using the two dimensional passwords, the same philosophy holds for them too, as n×n passwords are lengthy provided if all keyboard characters are allowed to involved then they become more complex and difficult to memorize. At one hand, the two dimensional passwords are lengthy and complex but the advantage they provide is tremendous in terms of password strength that is almost impossible to breach, in case these are sensibly used. The question arises whether we can use these passwords frequently. It is obviously infeasible to use these long and complex passwords frequently. But these passwords can effectively be used occasionally as a secondary one whenever there is a serious security threat to the system. In this way the benefits associated with these multidimensional passwords can be utilized. The following section describes the two-dimensional n×n password strength as compared to the linear passwords.

STRENGTH OF TWO-DIMENSIONAL PASSWORDS

To calculate the strength of the password, its entropy has to be calculated. Entropy is the amount of randomness of a password and is generally calculated as bits. If the password has N-bits entropy, then it can take up to 2^N attempts to break it through brute force method (Burr *et al*., 2006; Red Kestral Consulting, 2004; Allan, 2004). The formula for calculating the linear password entropy is generally stated as (Burr *et al*., 2006; Red Kestral Consulting, 2004; Allan, 2004).

$$\text{Password entropy} = \text{length}\times\log_2 m$$

$\log_2(m)$ is the bit entropy per character out of m possible character pool. In case of all possible keyboard characters i.e., the value of m would be 94 and entropy per character would be 6.55 bits. Length is the total number of characters in the password.

Let us consider the case of linear password that might allow containing any keyboard character. Let 'n' be the length of the password. Then the entropy of that linear password would be n×6.55 bits (Burr *et al*., 2006; Red Kestral Consulting, 2004; Allan, 2004). Now if we consider the two-dimensional password of n×n length and 94 keyboard characters provision, the entropy would be $n^2\times6.55$ bits (Safdar and Hassan, 2010; Safdar *et al*., 2010a). It can obviously be seen that moving towards multiple dimensional passwords increases the password entropy in terms of degree of the length times the entropy per character. In simple words, if N is the entropy bits for linear password then it would take 2^N attempts to break the password using brute force method, however, in case of two dimensional n×n password if entropy is N×n then it would take $2^{N\times n}$ attempts to break the password using Brute force method. Hence the strength of two-dimensional passwords would be much higher than normal linear passwords.

RULES OF FORMALIZING TWO DIMENSIONAL PASSWORDS

As mentioned above, the passwords should be n×n for the sake of simplicity. The following rules have to be followed:

- The password might contain all keyboard characters
- The password must contain at least one numeric, one capital letter, one small letter, one space blank and one special character

- The password is suitably being at least 8×8. However, the lower dimensions can be used contextually where ever required
- The passwords might be user selected or system generated or both as hybrid
- Permutations of user Id in passwords must be prevented
- Easy to use, dictionary words should also be avoided in passwords

PROPOSED METHODS OF USING n×n PASSWORDS

Two dimensional n×n passwords are always long and hard to remember so they might not likely be used frequently. On the other hand, these passwords are much stronger than the ordinary linear passwords. Hence to take the benefit of those passwords, these can be used occasionally as specialized secondary passwords whenever there is a security threat to the system or the system is in vulnerable state. This means the user must have one linear password preferably on NIST standards (Safdar and Hassan, 2010; Burr *et al*., 2006; Red Kestral Consulting, 2004; Allan, 2004) and one n×n password as special secondary password for secure login during vulnerable state of a system (Safdar and Hassan, 2010; Safdar *et al*., 2010a). Based on the formalization of n×n passwords, these passwords can either be selected by the user or can be auto generated by the system. Another potential way to select the n×n password is to compose it based on both user selection portion and server generated portion. This type of password selection is termed as hybrid password creation. Using n×n passwords is categorized in two parts i.e., password creation and applying password for authentication. Possible recommended methods of using n×n passwords are based on the way these passwords have been created. The proposed methods of using these n×n passwords are as following:

- Using a password created by a user
- Using a password generated by the server automatically
- Using a hybrid password i.e., User and server contribute to create a password

Out of the three proposed methods, first two are simple where as the third is hybrid in nature. It is also noticed that using long passwords effectively requires certain training of the users; hence all the above methods are meant for the trained user. The training of the users depends on the category of the user group and the complexity of the operations involved. Hence it is left to the organizations to target their special user groups whom they are willing to train and formalize the training themselves. Each of the above method is meant for the authentication in the following scenario as shown in the Fig. 2.

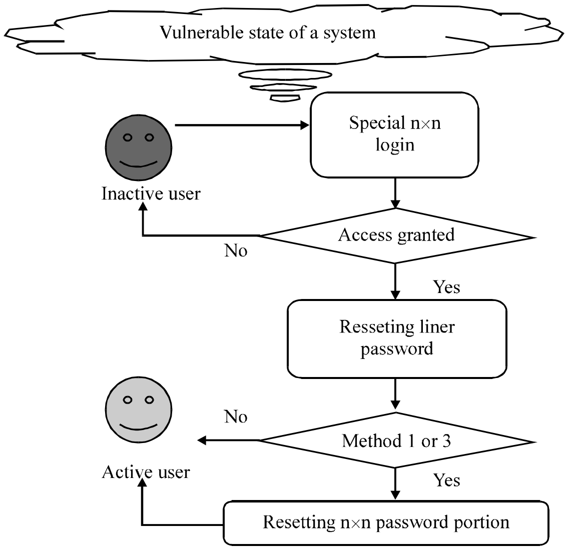

Fig. 2: Special login method in case of security threat to a system

As shown in Fig. 2, the user that is declared as inactive by the system under security threat is supposed to enter a special n×n password to gain its active status back. If the login fails, the user remains inactive and would be considered as threat to the system. However, if the special login succeeded and the method that is adopted is based on passwords created by user or hybrid passwords, then the linear password as well as n×n password would be reset either by the system or by the user depending on the methods adopted. On successful completion of the whole process, the user is considered as active user and gains a secured pass to the system. The following is the explanation of each method adopted for using n×n passwords effectively.

Method using password created by user: In this method the n×n password would be created/selected by the user at the time, the user account was made and is retained with the user. Usually the users created the passwords based on easy to remember dictionary words. NIST recommends avoiding using easy or dictionary words but to make passwords based on certain criteria as discussed earlier. It is recommended that the user create a password based on the NIST recommendations. The following steps have to be taken to apply the password effectively for authentication during unsafe state of the system:

- The inactive user is asked to provide the n×n special password
- If the login is successful, the user is then required to change the old linear password into the new one
- The user is also required to set new n×n password for future reference
- The status of the user becomes active and user can access system in a secured fashion
- Now user can login by using linear password all the time
- The above steps will be repeated if the system goes under threat again

Explanation: There are few issues associated to this method of using n×n passwords. As user has to create a password and retain it, hence the first issue that comes is to ensure that user may not create a password that is easy to breech. Therefore it is suggested to create a password based on NIST recommendations and try to avoid using easy dictionary words in passwords. Second major issue is related to memorizing those n×n passwords. As n×n passwords are long and complex so the user cannot possibly remember it all the time. In this case user may keep the password in written form with him. But it is also not practically feasible. One of the possible mechanisms to adopt in this case is the use of scratch card system that contains the code of accessing these stored passwords from online resources. Third issue is related to retaining the password for the long time. The password is created by the user and stored in the database to be retained there until it is not being used. This scenario will increase the probability of making more hacking attempts to steal that password. However, if the rotational reformation technique is applied to the password i.e., to store the password by rotating it to some angle (Safdar *et al*., 2010b) it might be saved much secure fashion. It is therefore recommended that in this method of using n×n password, the password created by the user must be in accordance with the NIST standards as well as to be stored using reformation technique as shown in Fig. 3.

Method using a password generated by the server automatically: In this method the system automatically generates the n×n password and transfers it to the user when the user requires it. The following step needs to be followed to use the password effectively under threat situation of a system:

- The inactive user is asked to enter the n×n password
- The inactive user requests the server to generate the n×n password

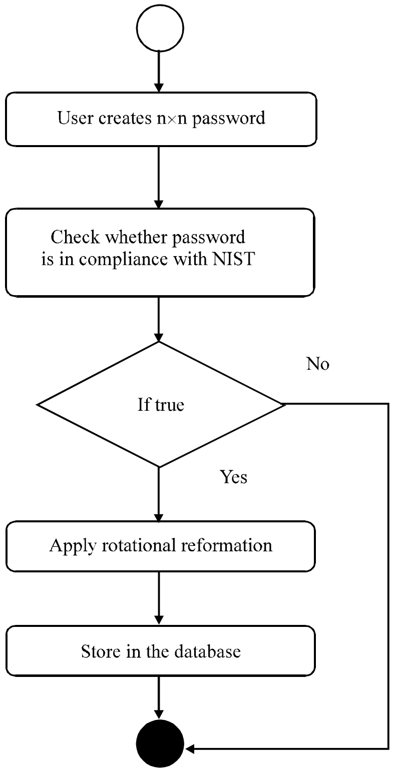
User creates n×n password
Check whether password is in compliance with NIST
If true
No
Yes
Apply rotational reformation
Store in the database

Fig. 3: Creation of the n×n password by user

- Server sends the newly auto generated password through secured channel to the inactive user via email or SMS. It may be noted that server will pick the email or cell number from the stored record rather than asking user
- On receiving the special password, the user enters the n×n Password
- When the login is successful, the user is required to change the old linear password to the new one
- The status of the user becomes active and user can access system in a secured fashion
- Access to the system is granted using linear password for every future reference
- The above steps are being repeated if the system goes under threat again
- The system generates a two-dimensional n×n password and transfers that to the user using secure channel when requested by the user

Explanation: As the method recommends that n×n password should be generated by the server automatically, therefore it can be deduced that the password will be strong. Hence it is not required to check whether it is in compliance with NIST standards as the nature of the passwords are automatically strong. This method of using n×n passwords also suggests that server should only generate the password once it is requested in the situation where the system is in threat. It can be deduced that the password will not be stored and retained in the database for the long period of time. In this way there is a less probability of hacking attack to steal such password.

Reducing the probability of hacking attack further, it is suggested that TTL (Time to Live) tag should be associated to the automatically generated n×n password. For ensuring more security, the passwords can be stored using rotational reformation technique. The user is not required to remember the password as it is generated dynamically once it is requested and then transferred to the user via some secured channel. The security of the password transferring media should be ensured using authentication certificates and security questions. The password creation in this method can be seen in the Fig. 4.

Method using a hybrid password: In this method the n×n password is partly been selected and retained by the user, however, the rest of the password is generated automatically by the system when requested. Based on this composition of the hybrid passwords, different symmetries such as diagonal, rectangle, diamond and checker box can be applied for handling the user and server portions. The following steps needs to be taken to use the password effectively:

- The inactive user is asked to provide the n×n password
- User requests the server to generate and provide the remaining portion of the password that user does not possess
- Server generates and transfers the required portion of a password through secured channel to the user
- User has been asked to enter the password in a dynamically generated symmetrical way such as diagonal, triangle, diamond or rectangle
- When the login is successful, the user is required to change the old linear password
- The user select new partial n×n password and retain it
- The user become active again and can login to the system with the new linear password
- The above steps are being repeated if the system goes under threat again
- The system generates the portion of two dimensional n×n passwords and transfers that to the user using secure channel when requested again

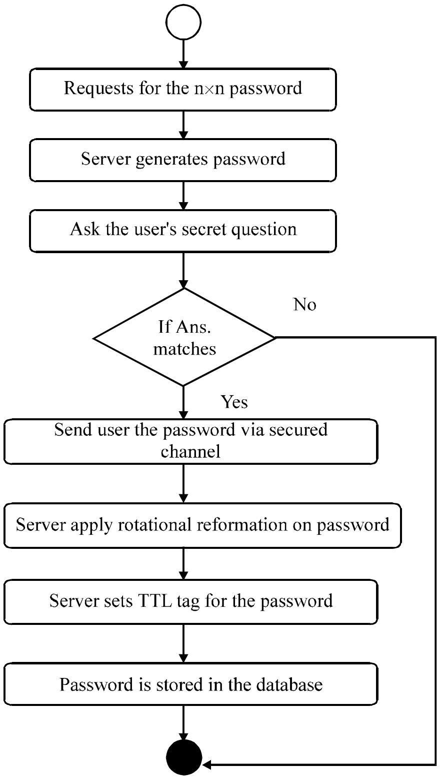
Requests for the n×n password
Server generates password
Ask the user's secret question
If Ans. matches
No
Yes
Send user the password via secured channel
Server apply rotational reformation on password
Server sets TTL tag for the password
Password is stored in the database

Fig. 4: Automatically Generation of the n×n password by Server

Explanation: This method recommends that a portion of the password should be created by user and retained by him as well as stored in the database. The server should generate the rest of the portion automatically at the time it is requested and when the system is considered in threat situation. This method of password creation makes n×n passwords stronger and almost impossible to be hacked. The reason is that if hacker manages to steal the password even then the complete password is incomplete, either the hacking done at user end or the server end. There is a processing overhead associated with this technique, as consolidating the two portions required an additional processing to be done. Proposed consolidation of the two portions of the passwords is based on the symmetrical distribution of the characters of the password for user and server portion. Few of the considered symmetries here are diagonal, diamond, checker and rectangle. This means that the server and user portion of the password is distributed almost 50 to 50% diagonally in case of diagonal symmetry. Similarly, the distribution of the two portions can be made using diamond, checker or rectangle. This implication of distribution symmetry enhances the strength of the password more as different symmetry provides different interpretation of the same password that is difficult to be guessed. This method requires the user to retain, the password portion created by the user, along all the time due difficulty to memorize lengthy and complex n×n password portion. Due to hybrid nature of the password, the creation of the password is done in two steps. First step is the one in which user create a password portion and this step is done at the time of user registration or every time user required to change the password. Second step is the one in which the server is requested to generate the portion of the password when the system goes under threat. Activities in first step can be seen in the Fig. 4. In Fig. 5 activity named, user create a portion of n×n password, follows he same sub activities as in Fig. 3 for creating the user portion of n×n password. Activities in second step can be seen in Fig. 6 where activity named, generate requested portion of n×n password, follows the similar sub activities as shown in figure 4 for automatically generating password of n×n password by server.

ANALYSIS OF THE PROPOSED METHODS

At one hand, if n×n passwords are long and complex but on the other hand they can be used occasionally rather than frequently. It is recommended that these passwords can be used under certain alarming situations as special secondary password. In the current scenario of the study if the system is under threat and it is wished to keep the system available to the customers, it is recommended to use n×n passwords. Therefore three methods are proposed for effectively using ▿ passwords to take maximum benefit from their strength making the user securely active in the vulnerable system. Let the three proposed methods be represented by the abbreviations as following:

- UCP: User Created Password
- SGP: Server Generated Password
- HP: Hybrid Password

Let the three methods be analyzed on the basis of probability of brute-force guess, probability of hacking and probability of losing a password. Table 1 shows the comparison of the three methods based on the mentioned factors.

Table 1 shows that method based on user created passwords suffer from high probability of being hacked and also there is a potential possibility of losing a password as it is retained with the user for a long period of time. Keeping this long and complex password secured with the user for a long period of time is still questionable.

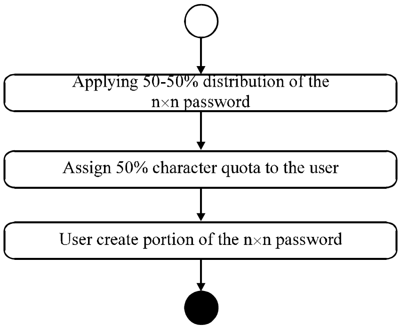
Applying 50-50% distribution of the n×n password
Assign 50% character quota to the user
User create portion of the n×n password

Fig. 5: Activities involved in creation of n×n password portion by user

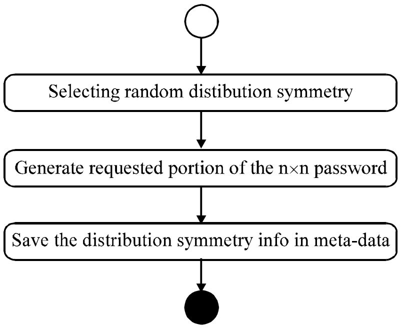
Selecting random distibution symmetry
Generate requested portion of the n×n password
Save the distribution symmetry info in meta-data

Fig. 6: Activities involved in generating n×n password portion by server

Table 1: Analysis of proposed methods

	Brute-force	Probability of hacking	Probability of password lost
UCP	NIL	High	High
SGP	NIL	Less than UCP	NIL if channel is authentic
HP	NIL	NIL	Equal to UCP

On the other hand if we observe the automatically generated passwords by server, probability of hacking is less than those of user created passwords. Also the probability of losing a password is nil as password is generated and transferred to the user when it is required only. In hybrid or mixed password composition, the hacking can be avoided at maximum as the two portions of the password are separately located. Hence it makes the probability of hacking in such a password equal to nil. The possibility of losing is still there as user retains a portion of that password but still it can be minimize using the proper management of those passwords. Now if the better method has to be selected, then one of the arguments is that it is always a contextual matter. As observed, if the user selects and keeps the special password for the long period of time. There is a fair chance for the user to lose a password either by misplacing it or misusing it resulting the hacking of that password. In the case where the complete password is to be generated by the server and then transferred to the user on request might also lead to lose the complete password if some hacking attempt becomes successful. However, in case of the hybrid solution, as the portion of the password is placed with the user and the rest is generated by the server so even successful hacking of server might not lose the complete password and vice versa. As all the passwords are n×n i.e., two dimensional in nature, therefore probability of using brute-force method to guess the passwords becomes nil in all of the methods. Considering all the methods on the parameters of brute-force guess, probability of hacking and probability of lost, it can be suggested that methods involved password creation by user is less likeable to adopt as compared to the other two methods. If we make sure of the secure channel to transfer the password to the user securely then methods in which server generate passwords and hybrid composition of passwords are feasible and much secured to adopt. It has also been observed that using hybrid method by incorporating different distribution symmetry enhances the strength of the password even more than the original (n^2×6.55). If the n×n passwords have been reformed rotationally before storing to the database, then it is likely to provide additional level of security from the outside hacking attacks.

Alsulaiman and El Saddik (2008) proposed a study for more secure authentication. For this purpose, proposed three dimensional passwords have been used. According to the study, three dimensional passwords are multifactor passwords that are not comprised of only one type of passwords. It is infact the composition of textual password, graphical password, biometric password and token based. The only base of calling these passwords as three dimensional passwords is that they have been implemented in the 3D virtual environment. That is, the password structure is not changed and is not extended to three dimensional space i.e., x, y and z plane. Moreover, calling this study as Three-Dimensional Secure Authentication is more appropriate rather than Three-Dimensional Password because the password structure for each type used in this study is the same as used conventionally. The results proposed by the study of Alsulaiman and El Saddik (2008) showed that user logins to the system by entering in to virtual 3D environment, then user may enters the area of textual password, if he/she wants to give that password than they may enter the linear textual password, then next 3D environment is open i.e., of biometrics. If user wants to ignore this biometric password than he or she can do that otherwise the biometric password is entered and the new environment is open to take another input and so on till all types of passwords used. This practice makes it unique combination or sequence of applying passwords that is only known to the user. The claimed authentication process is supposed to be stronger because it uses the phenomenon of using composite passwords with unique combination or sequence of applying them in the three dimensional environment. The provision of the combination increases the search space for the passwords and hence making them stronger when used in combination rather than to be used individually. As such the individual password strength is not enhanced as there is no change in the structure of the passwords.

In the proposed study, only textual passwords are considered. Textual passwords are suitable for all scale organizations from small to large scale. The small scale or medium scale organizations may not be able to afford the expensive hardware based solutions such as biometrics etc. Unlike Alsulaiman and El Saddik (2008) proposed three dimensional passwords without extending the password structure in three dimensional space, the proposed two dimensional n×n textual passwords in this study are extended to the two dimensional space i.e., x, y plane. This increases their strength tremendously in terms of bitwise entropy as well as permutations or scheme through which they have been applied. Moreover, due to defining these n×n passwords in two dimensions they are enabled of being interpreted in more than one way i.e., one n×n password has more than one interpretation i.e., row-wise interpretations or column-wise interpretations. In this way, if the password is leaked, it is not possible for the hacker to get its correct interpretation. These facts are completely missing in the work of Alsulaiman and El Saddik (2008) as the password used in their study is not extended to three dimension but the combination of conventional passwords are used in 3D environment. The properties associated with n×n passwords makes them usable in much more secure fashion even in the vulnerable state of the systems. n×n passwords are long and complex and hence they should not be used as the passwords for normal daily life authentication but to be used only in alarming situations (Safdar and Hassan, 2010) such as the system goes under vulnerable state due to some threat. This approach is not aimed by Alsulaiman and El Saddik (2008) in their study and user may be annoyed using long login method in 3D environment. Unlike Alsulaiman and El Saddik (2008) the proposed methods of using the n×n passwords aimed for the situation when the system is intruded by the threat and it is desired to keep the system workable. Hence the defined three methods in this study that are based on n×n passwords can be used smartly and effectively to get maximum benefits out of them. The results of the current study cannot be addressed by Alsulaiman and El saddik (2008) study. The idea of using n×n passwords in hybrid approach is unique and provides extra layer of security by the provision of different shape structure at user interface level.

CONCLUSION

There are methods to use long and complex passwords in such a way to acquire maximum benefit by managing them effectively. As n×n passwords are not supposed to be use frequently, hence it limits the problem of memorizing them all the time. The study proposes the methods of using strong password, when the system goes under threat and the special authorization can be provided to the potential users to continue their work in the alternate secured environment. All of the methods let us use n×n passwords effectively in different contexts wherever it is applicable. These methods provide us with the mean of proper management of two dimensional n×n passwords. This study not only depicts the importance and strength of two-dimensional passwords but also describes the issues associated with the two dimensional passwords. This effort makes it possible to understand that passwords can exist as multi-dimensional and let us do further study on the passwords that can be multidimensional in nature. The proposed methods contribute in the scenarios where, there is a special and secure requirement of authentication. The study also contributes special authentication services in the area of providing services availability in a secured fashion to the end user when the system is under attack.

REFERENCES

Allan, A., 2004. Passwords are near the breaking point. Gartner Inc. http://www.indevis.de/dokumente/gartner_passwords_breakpoint.pdf

Alsulaiman, F.A. and A. El Saddik, 2008. Three-dimensional password for more secure authentication. IEEE Trans. Instrumentation Measurement, 57: 1929-1938.

Burr, W.E., D.F. Dodson and W.T. Polk, 2006. Information Security. NIST Special Publication, Gaithersburg, MD.

Florencio, D. and C. Herley, 2007. A large scale study of web password habits, WWW 2007/ Track: Security, privacy, reliability and ethics. Proceedings of the 16th International World Wide Web Conference, May 8-12, Bnaff, Alberta, Canada, pp: 657-665.

Gaw, S. and E.W. Felten, 2006. Password management strategies for online accounts. Proceedings of the 2nd Symposium on Usable Privacy and Security SOUPS 2006, July 12-14, Pittsburgh, pp: 44-55.

Helkala, K. and E. Snekkenes, 2009. Password generation and search space reduction. J. Comput., 4: 663-669.

Hsueh, S., 2008. Database encryption in SQL server 2008. Enterprise Edition, SQL Server Technical Article. http://technet.microsoft.com/en-us/library/cc278098%28SQL.100%29.aspx.

IBM ISeries, 2009. Digital certificates for user authentication. IBM iSeries Information Center. http://publib.boulder.ibm.com/iseries/v5r1/ic2924/index.htm?info/rzahu/rzahurzahu4aeauthenticatewcerts.htm.

Li, C., Y. Wang and L. Liu, 2009. A biometric templates secure transmission method based on bi-layer watermarking and PKI. Proceedings of the International Conference on Multimedia Information Networking and Security, Nov. 18-20, Hubei, China, pp: 95-98.

Oorschot, P.C.V. and J. Thorpe, 2008. On predictive models and user-drawn graphical passwords. ACM Trans. Inform. Syst. Secur., 10: 1-23.

Red Kestral Consulting, 2004. Random password strength. http://www.redkestrel.co.uk/Articles/RandomPasswordStrength.html.

Safdar, S., M.F. Hassan, M.A. Qureshi and R. Akbar, 2009. Biologically inspired execution framework for vulnerable workflow systems. Int. J. Comput. Sci. Inform. Secur., 6: 47-51.

Safdar, S. and M.F. Hassan, 2010. Moving towards two dimensional passwords. Proceedings of the International Symposium on Information Technology ITSIM 2010, June 15-17, Malaysia, pp: 891-896.

Safdar, S., M.F. Hassan, M.A. Qureshi and R. Akbar, 2010a. Framework for alternate execution of workflows under threat. Proceedings of the 2nd International Conference on Communication Software and Networks, Feb. 26-28, Singapore, pp: 218-222.

Safdar, S., M.F. Hassan, M.A. Qureshi, R. Akbar and R. Aamir, 2010b. Authentication model based on reformation mapping method. Proceedings of the International Conference on Information and Emerging Technologies, June 14-16, Karachi, Pakistan, pp: 1-6.

Smith, R.E., 2002. The Strong Password Dilemma. Chapt. 6. Addison-Wesley, New Jersey, ISBN: 0-201-61599-1.

Tan, S., H. Zhu and Y. Wang, 2009. Some notes on password authenticated key exchange based on RSA. Proceedings of the International Conference on Computational Intelligence and Security, Dec. 11-14, Beijing, pp: 580-583.

Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy and N. Memon, 2005. Authentication using graphical passwords: Effects of tolerance and image choice. Proceedings of the Symposium on Usable Privacy and Security, July 6-8, Pittsburgh, pp: 1-12.

Yang, D. and B. Yang, 2009. A new password authentication scheme using fuzzy extractor with smart card. Proceedings of the International Conference on Computational Intelligence and Security, Dec. 11-14, Beijing, pp: 278-282.