User Authentication using Musical Password

Naveen Kumar
School of Computer and
Information Sciences,
IGNOU, Maidan Garhi,
New Delhi, India.

ABSTRACT

Computers, Mobile and other handheld devices depend largely on passwords mechanism to identify and authenticate users. Typically, passwords are strings of characters and digits. Alphanumeric passwords are convoluted to remember for users because a safe password should be long and arbitrary, however users pick short, simple, and insecure passwords. Different solutions have been proposed to aim to make passwords more memorable and easier for users to use and, for this reason, it is more secure. In this paper, we propose a new user authentication scheme, based on the principle that the music, melody can all aid memory. In this scheme the simulation of Piano instrument is implemented for proof of concept. User creates the music using the keys of Piano simulation, which will be stored as user password in the secure database. Each key selection of piano can be associated with a unique secret code, the combination of these codes are actually stored in the database after hashing, which will be tested at the time of user authentication. The proposed scheme is highly memorable, defiant to brute force attacks and dictionary attack, protected from shoulder surfing attacks and from spywares tracking. This combination of security and usability will be a focus for users to choose this scheme for their web, computer and mobile passwords.

Keyword: Security, User Authentication, usability, memorability, Password, Musical Password.

1. INTRODUCTION

Computer and network security has been formulated as a technical problem. However, it is now widely recognized that most security mechanisms cannot succeed without taking into account the user [1]. Users are asked to remember a growing number of passwords for computers, emails, and online financial services. We refer to the security and usability problems associated with alphanumeric passwords as "The password problem" [2]. Managing these security requirements is virtually impossible for users. Consequently, users ignore the requirements, leading to poor password practices. This problem has led to innovations to improve password schemes. Human memory is not only assisted by vision but also by sound, taste and smell. The most important amongst these is the sense of hearing. In daily life we tend to remember music of songs, which we may have heard long, time back. As per various studies, it is found that the power of music to affect memory is quite intriguing. Mozart's music and baroque music, with a 60 beats per minute beat pattern, activate the left and right brain. The simultaneous left and right brain action maximizes learning and retention of information [3]. Music has been shown to improve memory in several situations. In one study of musical effects on memory, visual cues (filmed events) were paired with background music. Later, participants who could not recall details of the scene were presented with the background music as a cue and recovered the un-accessible scene information [4]. This suggests that sound or to be specific music is a very important tool for memory retention. It is a very common practice amongst students to remember their course work using music as an aid. These results and facts motivate to use the strong memorability characteristics of music in developing an alternative mechanism for user authentication.

2.ALTERNATIVES AUTHENTICATIONS

All user authentication schemes are based on three fundamental pieces of information: what you know, what you have, and who you are [5] which, also corresponds to token-based authentication, knowledge-based authentication and biometric authentication. For proving who they are, users can provide their name, email address, or a user ID. Since this information provides no assurance of identity, some system operators are beginning to employ biometrics (such as fingerprints, voice recognition, iris scans, or retinal scans) as methods of user identification. For proving what they have, users can produce service cards (i.e., ATM cards), physical keys, digital certificates, smart cards etc) [6]. For proving what they know, users can provide a password or pass phrase, or a personal identification number (PIN). This information is essentially a secret that is shared between the user and the system however; also have drawbacks, most notably in terms of memorability and security.

One recent innovation in knowledge-based authentication is visual or graphical passwords, i.e., passwords that are based on images rather than alphanumeric strings. The basic idea is that using images will lead to greater memorability and decrease the tendency to choose insecure passwords. This, in turn, should increase overall password security. Some usability studies have shown that graphical or virtual passwords have significantly large password spaces [7].Until recently the security problem has been formulated as a technical problem. However, it is now becoming widely recognized that security is also fundamentally a human–computer interaction (HCI) problem [8]. Audio signal are one of the most useful and effective features for user authentication in mobile environments. Some user authentication schemes are being developed using audio and voice signal. Comparative analyses of these audio based schemes are as shown in the Table 1. Today other methods, including biometrics and smart cards, are possible alternatives. However, passwords are likely to remain dominant for some time because of the drawbacks of reliability, security, or cost of other technologies. In particular, smart cards also need PINs and passwords.

Table 1. Comparative Analysis of Audio-based Authentication Schemes

User Authentication Scheme	Usability		Security
	Authentication process	Memorability	Possible attack Methods
Audio Authentication (Voice system and Voice Verification)	Voice signal work as password, voice may be speech or any audio. Process can be fast or slow depend on user.	Depends on the Voice password. Long and random passwords are hard to remember, but long song are easy to member.	Dictionary attack, Brute force search, Guess, spy ware, Shoulder surfing, etc.
Audio and Image Authentication	Images can be associated with a particular piece of music as a password.	The Images and music association. Number of associations chosen by user improve security but reduce memorability.	Brute force search, Guess, spy ware, Shoulder surfing, etc.
Audio-Visual Person Authentication using Speech and Ear Images	The image of ear shape of a user is integrated with user speech information, which increases the robustness of user authentication.	Not Applicable. Comes under the biometrics user authentication.	Speech is deteriorated by acoustic noises and time. Ear shape feature changes with time.

3. MUSICAL PASSWORD SCHEME

The primary inspiration is that, using music will lead to greater memorability and decrease the tendency to choose insecure passwords because human's ability of musical memory is much more powerful than the textual memory [9] [10]. A case study on an expert pianist, researchers Chaffin & Imreh (2002) found that a retrieval scheme was developed to guarantee that the music was recalled with ease [11]. However, any musical devices can be used to enter a musical password, a simulation of piano instrument is preferred in this paper where user press the keys of the piano to create the music and consequently the password. Aim of proposed scheme is to let the user use a musical note as a password. An end user uses a password of length 8-10 characters. Using a musical password this length can be increased to 80-100 characters. This scheme is also protected from shoulder surfing attack as intruder may listen to the tune yet not aware of the correct piano configuration or the keys. Only the tempo of the tune can be inferred from the tune not the keystrokes. Also, every time the Piano window position is changed to reduce the mouse tracking spywares and shoulder surfing attack.

The password is created with the number of keystrokes pressed for making the music. Every key in the piano is associated with the unique secret code. The basic mapping table as shown in Table: 2, which stores secret codes associated with the basic piano keys is stored in a database. If multiple keys are selected by the users, bit wise AND & bit wise OR operations are used for White keys + Black keys (dissimilar) and White + White or Black + Black keys (similar key) selections respectively. Further, these respective bit-wise codes will be converted into the ASCII codes for temporary processing. These secret codes are not known to the users, and used for providing the resistance from the shoulder surfing attack. User creates the tunes or rhythms and listen the music, however this music generated by the user is not stored. Only the output string generated with the keys secret codes will be stored in the database in the hashed form. The input device for interactions with piano can be a mouse, keyboard or styles. For example, consider a user create the basic tune for "Twinkle -Twinkle little stars…" and press the keys "DDAAGGFAAGGF", the music generated by the keys will be and temporary stored for till the login window is open for user confirmation. The actual password which is formed is "Lg@8Lg@8N1kSN1kSV7x8V7x8M0#qN1kSN1kSV7x8 V7x8M0#q".

Table 2. Basic mapping of Piano keys and Secret Code

Key	Secret Code	Key	Secret Code
C	J$2k	B	5drS
D	Lg@8	C	X29b
E	hC7a	#C	Us3l
F	M0#q	#D	J17C
G	V7x8	#F	Gjr6
A	N1kS	#G	ZA56
		#A	$#ql

The password string generated can be very long, difficult to remember but this is nothing to do with the user. Also, the hash function covert these strings into another form for secure storage.

4.ALGORITHM: PROPOSED SCHEME

The algorithm has three main phases, first is Music Password Creation Phase where user will create the music, next is Password Storage Phase in which user password will be store secretly and the last phase is Password Verification Phase, where user have to generate the same music which user had created at the time of Password Selection Phase. These phases are further explained as below

4.1 Password Creation Phase

1. User selects a music instrument from the instrument gallery provided by the server like piano, guitar, etc.
2. After entering of user name, to create password system record the sequence of the keys or user's actions towards the selected octaves in the virtual instrument. As shown in Fig 1, where user has selected Piano instrument.
3. Link list is formed in which each node will have secret code for one key selection or action on the music instrument.
4. Recording continues till the user clicks to finish Password Selection Phase.

4.2 Password Storage Phase

1. The whole link list is passed to the temporary buffer where padding and appending of length is done before sending it as an input for MD5 algorithm.
2. 128-bit sequence is generated by MD5 algorithm and stored in the database corresponding to each users.

4.3 Password Verification Phase

1. After entering the correct username, user need to select a virtual environment from the virtual art gallery provided by the server.
2. User selects a music instrument through which password was created. User needs to generate the same rhythm or tune using key sequence or actions as done in password creation phase.
3. This new linked list link list is passed to the temporary buffer where padding and appending of length is done and sent as an input for MD5 algorithm.
4. The new MD5 128 bit string is compared with the 128 bit MD5 value stored in the database, if any matching is there login will be successful else not.

5. SECURITY ANALYSIS

There are many aspects of security analysis like evaluating a system against common password security issues, the main issues we have focused are brutal force attack, dictionary attack, problems which shoulder surfing attack and spyware programs that runs in the background, recording all the mouse or key strokes. In this paper we have analyzed musical password scheme against these security problems.

5.1 Brute Force Attack

The main defense against brute force search is to have a sufficiently large password space. It is more difficult to carry out a brute force attack against musical passwords than graphical passwords and also alphanumeric passwords. A standard Piano has 88 keys, 54 are white and 36 are black. The password space of text password is 96^N, where 96 are printable characters and N is the length of password, Generally the password length is 8 characters. In case of Piano of 88 keys and use of 10 fingers, may lead to the password space ($^{88}C_{10}$)^N, and unlikely to the text password here the N is quite large normally it is 50-60 size. However, the exact calculation may be different, if multiple keys are pressed together. The information of a password space defined by Fabian Monrose [12] is as "the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose". It is a measure that determines how hard the attack is. However, trying to have a scheme that has very large possible passwords is one of the important parts in resisting the attack on such a scheme. We noticed that by increasing the number of keys in the Piano instrument password space increases exponentially.

5.2 Dictionary Attacks

Since this scheme involve only the music it will be impractical to carry out dictionary attacks or automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area. Overall, we believe musical passwords are less vulnerable to dictionary attacks than other password schemes.

5.3 Spyware Attacks

As mouse input can be used to create the password key-logger spyware software may not be used to break musical password. Due to different musical environment, mouse-tracking spyware will also not be an effective tool against virtual password. Also, mouse motion alone is not enough to break musical password. Such information has to be correlated with application information, such as timing information.

5.4 Shoulder Surfing Attack

As the most of the rhythms are generated using the multiple key selection, which itself deceive the shoulder surfing attacker, however as second layer of defense a mapping table is used which contains secret code associated with each piano key as already given in Table: 1. These secret codes may be given by the users and may differ from user to user.

6. EXPERIMENTAL RESULTS

As a proof of concept we have taken a musical instrument Piano that consist of 8 white and 5 black keys. However, the standard Piano should be of 52 white keys and 36 Black keys. User can perform either selection or action on these objects, as a part of their virtual password. About 32 users have tested the experimental environment including 10 female and 22 males of computer science graduation. Musical Password mainly has two windows Login Registration and Login Verification.

6.1 User Registration

Musical password registered the first time users with their proposed user name, instrument selection as given in the *Figure: 1.* In this after entering the user name user selects a musical instrument from the instrument gallery provided by the server. On click of *Password Creation* button, system records the sequence of the user's key selections or actions towards the selected musical instrument. As soon as password is stored in the database, user Login button appears to proceed.

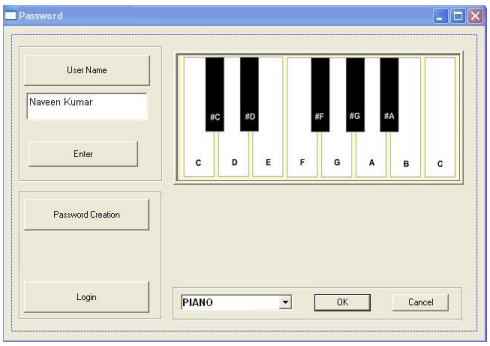

Fig. 1: Password Creation Phase

6.2 User Verification

The registered users enter their selected user name if correct than, user have to choose a musical instrument from the list of instruments as shown in Figure 2. Next, user needs to repeat the same tune or rhythm and key selections on the musical instrument as done in registration process. System calculates, the MD5 value based on the given input values of the user if it is same, user is successful.

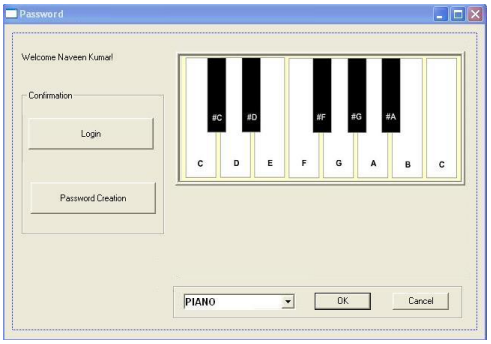

Fig. 2: Musical Password window for User Verification

7.CONCLUSION

Alphanumeric password scheme is inherently insecure as these are subject to a tradeoff between usability and security, however alphanumeric scheme remain popular as their

concept corresponds to an existing common model worldview making them an easy to understand concept. Many different schemes have been used in specific fields like smart card, fingerprint authentication etc. Other schemes are under study yet they have never been used in the real-time. The motivation of this work is to have a scheme that has an enormous password space. In this paper, we have proposed a user authentication scheme based on musical instruments. As the rhythms and songs are highly memorable and get stored in human Long Term Memory, to take advantage of this feature user password can be a combination of user interactions and inputs towards the musical instrument in order to generate a tune. System repeats the reverse process for verifying the user identity. Implementing the familiar musical instrument, objects and actions for the multiple users is a critical task, which can be a part of further study. Also, there is a need to explore the other attacks on the system like viability of shoulder surfing attack in case the user is not using the headphone. The musical password is now in its infancy. A study on a large number of users is required. The main application areas of Musical Password are systems such as Online services, Banking services, and critical servers can be protected by Musical Password system with large library of complete musical instruments. Moreover, its applications over mobiles, handheld devices and ATM machine may be explored.

8. REFERENCES

[1] Daniel K., 1990. "Foiling the Cracker: A Survey of, and Improvements to, Password Security," Proceedings of the 2nd USENIX Unix Security Workshop, pp. 5-14.

[2] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, 2005. "Authentication using graphical passwords: Basic results," Human-Computer Interaction International (HCI 2005). Las Vegas, NV.

[3] Neverman. 1999 The Affects of Music on the Mind. On-line. Internet. 20 December 1999. Available http://www.powell.k12.ky.us/pchs/publications/ Affects_of_Music.html, Last accessed in October 2012.

[4] Boltz, M., Schulkind, M., and Kantra, S., 1991. Effects of background music on the remembering of filmed events. Memory and Cognition, 19 (6), 593-606.

[5] S. Brostoff, and M.A. Sasse, 2000. "Are Passfaces more usable than passwords: a field trial investigation," People and Computers XIV—Usability or Else, Proceedings of HCI, Springer, Berlin, pp. 405–424.

[6] http://www.rsasecurity.com/products/securid/, Last accessed in October 2012.

[7] Kumar Naveen. 2011. Password in Practice: an Usability Survey. Journal of Global Research in Computer Science, Volume 2, No. 5, pp. 107-112, ISSN-2229-371X.

[8] J. Thorpe, and van Oorschot, 2004. "Towards secure design choices for implementing graphical passwords," ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), Washington, DC, USA, Vol. 3, pp. 664 – 666.

[9] Samson, S., Zatorre, R.J. 1991 Recognition memory for text and melody of songs after unilateral temporal lobe lesion: evidence for dual encoding. Journal of Experimental Psychology: Learning, Memory, and Cognition. 17(4), 793-804.

[10] Wallace, W. T., 1994. Memory for Music: Effects of Melody on Recall of Text. Journal of Experimental Psychology: Learning, Memory, and Cognition, 20 (6), 1471-1485.

[11] Chaffin, R., Imreh, G. 2002. Practicing perfection: piano performance as expert memory. Psychological Science. 13 (4), 342-349.

[12] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin, 1999 "The design and analysis of graphical passwords," Proceedings of the Eighth USENIX Security Symposium, pp. 1–14.