IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Strengthening the ATM-User Authentication Using Pass Pattern System

B. Rajmohan[1], Punyasloka Parida[2] and A. Vivek Anand[3]

[1,2,3]Department of Information Technology, Adhiparasakthi Engineering College, Melmaruvathur, Tamil Nadu, India

Abstract

The more the technology improves, its complexity increases too. ATM machines have reduced bank's long queues and indeed proved to be a valuable luxury, but it stays valuable as long as the user's money is secure. In this paper, this system presents a unique technique that can replace the contemporary ATM PIN system to authenticate a user. This technique is called PassPattern System (PPS). This is a dynamic password scheme that helps the user to remember multiple passwords (ATM PINs in this case) with ease and also strengthens the authentication. This technique is based on the idea that users can remember a pattern easily than a string of characters. Therefore the user has to remember the pattern rather than his PIN. The PIN changes every time according to the pattern. The positions which make his pattern contain randomly generated characters. These characters constitute to be his ATM PIN for that particular time. This dynamic scheme can be implemented in existing infrastructure without creating the need of any extra equipment. Therefore, this scheme provides the user with security and user-friendliness without compromising user's comfort.

Keywords: PassPattern System, Security Attacks, ATM Authentication.

1. Introduction

Man always tries to build machines which provide him comfort in both ways – physically and mentally. This sort of convenience is obtained when his machine is driven with changing technology. As said by Tobey Maguire in the movie spider-man "*With great power comes* great responsibility", technologists too hold a big responsibility in building machines which eases the life of common man, while being concerned about its future outcomes. Hence, when technology improves, security always remains a matter of concern. Automated Teller Machine (ATM) is solely responsible for reducing the long queues in the banks and thus giving an inexpensive comfort. But its contemporary password system also has some kind of demerits. A different password scheme called PassPattern System (PPS) overcomes the obstacles faced by the contemporary PIN system in ATMs.

2. PassPattern System

PassPattern System is a dynamic password scheme which is based on the idea that "Human can remember and identify a pattern or shape easily than bunch of characters". A system which uses PassPattern System (PPS)[1] needs to authenticate its user by a pattern rather than the password. The System generates an N X N matrix of blocks or cells, which is known as PatternSquare. Now this PatternSquare contains a random character, number or a special character in each cell. The content of the PatternSquare changes each time the user logs in. At the time of the registration the user needs to select a sequence of positions, which in actual is his password. These positions form his pattern and when the machine authenticates him, he needs to choose those positions. The characters in the pattern form his password for that particular time. The characters in the matrix change dynamically during the next login.

Consider the figure given below. It is a sample PatternSquare. The cells with grey background form a pattern

P	W	@	]	}	&	#
K	N	B	3	2	M	b
^	%	*	p	k	L	J
N	J	H	1	;	\	?
<	=	-	_	!	A	o
T	R	X	Z	M	~	9
6	1	O	t	a	l	k

Fig.1 Sample PatternSquare

The characters in the pattern form the password. Well, this is too lengthy. Let us consider fig. 2 which has a smaller pattern.

P	W	@	]	)	&	#	R
K	N	;	3	2	"	^	%
^	%	*	p	K	,	J	B
N	J	H	1	X	\	?	>
<	=	-	_	!	A	L	V
T	R	:	Z	M	~	9	0
6	f	3	t	a	l	k	s
c	z	m	b	j	r	x	w

Fig.2. A sample PatternSquare

Now the user's pattern is the shaded regions in the PatternSquare. This type of system is also called as challenge-response system. The PatternSquare is a challenge given to the user and the user gives a response by selecting the correct pattern.

3. PassPattern System in ATMs

The Authentication system used in ATMs is the contemporary PIN system. This PIN based system is a secure system, but it has its own demerits. So bringing the PPS in ATMs will strengthen the user authentication without changing the existing infrastructure. For example, if State Bank of India plans to authenticate its ATM users by checking their finger prints, it needs to install the machine to check fingerprints in its each and every machine. In other words, it has to upgrade its infrastructure, which increases the cost and complexity. Using PPS all it needs to do is change the underlying software without changing the existing infrastructure.

The ATM screen displays a PatternSquare of N X N matrix. The user can select the characters in the cells which make his pattern by touching them on the screen. This way user can manage to have a secure transaction every time without having the burden to remember the password. This also relieves the user from getting confused with other PINs, if the user holds multiple bank accounts.

4. Designing the PassPattern System

To build a PPS, one need four components – a PPS Software, Random number generator, Image generator and database. The software controls both the random number generator and the image generator. The PassPattern database stores the PassPatterns of the users. In the database the PassPatterns are indexed in row-major order, starting from 0 to $N^2 - 1$ (where N is the size of the matrix).

The block diagram of registration process in a PPS is given below

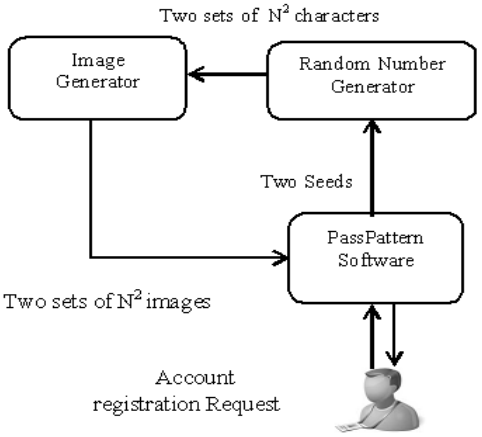

Fig.3. Block Diagram of Registration Phase - 1

When a user makes a registration request (The Bank does this in behalf of the ATM users), the PPS software generates two seeds and gives as an input to the random number generator. The seed is generally an initial value given to a random number generator, which generates random number based on that value. The Random number generator generates two sets of N^2 characters which are sent to the image generator and the image generator generates two sets of PatternSquares. The user has to select the pattern by choosing the characters in those positions. The reason behind generating two images is that the user has to reconfirm his pattern by selecting those positions again. The user has to give these two secret codes and his account number or user name to PPS software again. Now the PPS software generates seeds according to the input code give and sends it to the random number generator. The random number generator generates two sets of N^2 characters and this is verified with the input. If this happens to be same, then the PPS calculates the MD5 Hash of the username and PassPattern and stores them in PassPattern database.

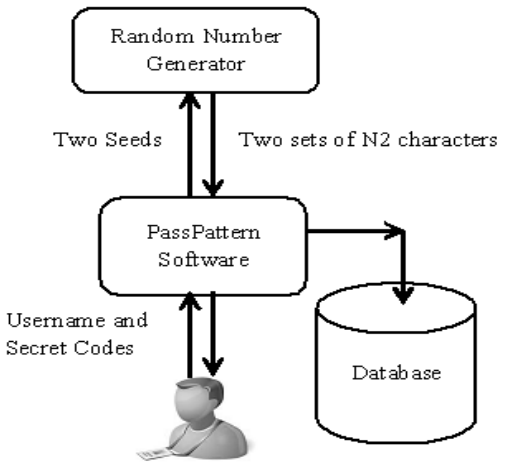

Fig.4. Block Diagram of Registration Phase – 2

During User Authentication, the user has to swipe his card in the ATM machine which in turn displays a PatternSquare. Now user has to choose his/her pattern which is sent to thePassPattern software. The PassPattern software now calculates the MD5 Hash of user name and PassPattern and verifies it with the data in the database. If it happens to be correct, user gets the permission to make transactions or else the user is rejected.

The PassPattern verification in ATMs can be strengthened by increasing the size of pattern square. More the size, higher will be the security. The number of possible patterns of length n will be $(N^2)^n$. Hence, the complexity and security increases with the size.

5. Hiding the PassPattern Square using image.

The above sections described about how to authenticate a user and how the system works. This section is about an additional feature that can be added to the PassPattern System. The PassPattern authentication can be strengthened by overlaying an image on the PatternSquare[2][3]. The PPS Software will generate the pattern, but it will be hidden under the image. Hence, by touching the particular portion of the image, the user is selecting a position in the hidden PatternSquare. This is kind of technique is depicted below.

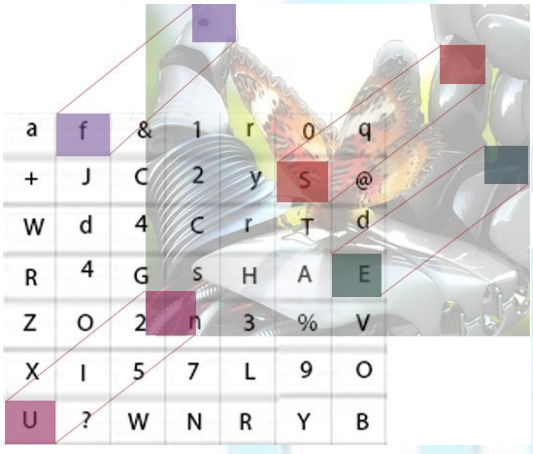

Fig.5. Selecting the position in the PatternSquare by touching the particular portion of the image.

In the above given image, touching the finger tip of the robot's hand selects 'f' in the hidden pattern. Now the pattern itself is hidden and the user has to remember the portions of the image. This could be made user friendly, if the user has a familiar image in the ATM Screen. Images like the user's own photo or his car makes the challenge simpler for the user. This Technique too has its own demerits, like if the user accidently touches a portion that belongs to the other cell, it could lead to incorrect password generation. Though this method has a mild flaw, it enhances the user's security, especially form *shoulder surfers.*

6. Attacks that PPS can overcome

ATM users are liable to face bad consequences when their ATM card falls in wrong hands. In normal contemporary user authentication scheme, ATM users have to bear the consequence, if the card is stolen or misused. In PPS, user need not have to look for such consequences due to its dynamic password generation. It is much more secure than the contemporary system attacks such as Brute force, Dictionary attack, Key logger and Shoulder surfing.

5.1 Brute force Attack

In Brute force attack the hacker (Who steals your ATM Card) can use two techniques. First, he can simply choose some bunch of characters from the PatternSquare ignoring the pattern. For Example, if the hacker needs to crack a four digit PIN, he would have to select those four from the 94 printable ASCII codes (Take for an instance that the characters used by the PPS in ATM machines uses ASCII Codes). So the probability of success is $1/(94)^4$.If the guess goes wrong, the probability of success will be the same for the next trial, as the PPS generates a new bunch of characters every time. This makes the cracking process almost impossible. The other way of breaking the system is trying out all the possible combinations of positions. For example, if the user considers an 8 X 8 PatternSquare there will be 64^n or ${}^{64}P_n$ different patterns of length n. The 64^n combinations are possible if a position is repeated in the pattern, otherwise the number of combinations is ${}^{64}P_n$.So for N X N matrix, Number of possible patterns $(N^2)^n$, if the positions is repeated or else, it is $N^2! / (N^2\text{-}n)!$ So this would take enormous amount of attempts to break the image. Thus the hacker would prefer to drop down this idea.

5.2 Key loggers

Key logger is a program which captures the user's key strokes. The information gathered by the program is sent to the hacker. As PPS has a dynamic password scheme, the key strokes changes every time the user gives his PIN because of the change in characters in the PatternSquare. So this leaves the hacker inefficient to track the PIN.

5.3 Dictionary Attack

Dictionary attack is a type of attack where the password can be cracked by attempting the strings written in the list of possible passwords called dictionary. This method is efficient when user use very simple Passwords or PINs. But PPS, due to its dynamic scheme is highly strong against Dictionary attacks. It can be cracked only if

common shapes are used, but this too can be prevented if a system of dynamically changing pattern is used.

5.4 Shoulder Surfing

Shoulder surfing is peeping at others passwords or more precisely, looking over other's shoulder to gather information on user's PIN[4]. This always happens in crowded ATMs or at any public place. But Shoulder surfing never works in PPS. The shoulder surfer would be puzzled looking at new password every time the user logs in. Shoulder surfing can also be done at a particular distance by using binoculars, but such shoulder surfing will leave the hacker more confused as it changes dynamically. This is the strength of Dynamic scheme, which minimizes the cost and is user-friendly too.

7. Conclusions

The PassPattern System is a cost-efficient, user friendly technique, which due its dynamic property helps to build a secure system which can be implemented in ATMs. This System can be implemented anywhere irrespective of the geography and infrastructure. The PPS overcomes the problems faced by the contemporary password techniques and helps to build a system without compromising user's comfort. So Bank ATMs can strengthen their security by adopting this technique. As this technique can be built up in the existing infrastructure, the cost for up gradation would be minimal.

References

[1] T. Rakesh Kumar, S. V. Raghavan, PassPattern System (2008).
[2] T. Morkel, J.H.P. Eloff, M.S. Olivier, an overview of Image Steganography.
[3] Suo, X., Owen, Y.Z.: Graphical Passwords: A Survey in: 21st Annual Computer Security Applications Conference.
[4] Brainard, J., Juels, A., Rivest, R.L., Szydlo, M., Yung, M.: Fourth-Factor Authentication: Somebody You Know. In: Proceedings of the 13th ACM conference on Computer and communications security, pp. 168–178 (2006)
[5] Shepard, R.N.: Recognition memory for words, sentences and pictures. Journal of verbal Learning and verbal Behavior 6, 153–163 (1967)