MIRAGE 1.0: A Key Entry Scheme Resilient to Shoulder Surfing

Chaitanya Srinadhu
GITAM University
Dept. of Information Technology, GITAM University, Visakhapatnam, India-530016

Sree Kashyap Addanki
GITAM University
Dept. of Information Technology, GITAM University, Visakhapatnam, India-530016

B.V.R.K. Ram Acharyulu
GITAM University
Dept. of Information Technology, GITAM University, Visakhapatnam, India-530016

ABSTRACT
Two level authentication systems are widely being used in many ATM's (automatic teller machine).To be more illustrative they are now crust of the security systems in many military agencies. It is very often noticed that, a combination of biometric and key login or a combination of token and a key are widely accepted authentication systems. Besides the problem of high faulty recognition, biometric suffers from a backdrop of high cost and slow authentication process. Like many of our valuable possessions tokens like magnetic cards are highly prone to theft and duplication. Traditional key entry schemes are very much vulnerable to peeping and shoulder surfing attacks. Furthermore, with the advancement of technology many other fake login schemes like dictionary attacks or key logging have become a major security concern. In this paper we propose pattern based key entry scheme, Mirage 1.0, which would not only withstand peeping and shoulder-surfing attacks but also would be resilient towards dictionary attacks and key logging schemes.

General Terms
Counter measures of shoulder surfing, pattern based key entry scheme, shoulder surfing.

Keywords
Biometric authentication ,Key logging ,shoulder surfing, MIRAGE 1.0.

1. INTRODUCTION
Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running in a device. This is an important process which assures the basic security goals, viz. confidentiality and integrity. Also, adequate authentication is the first line of defence for protecting any resource. With the rapid growth of internet based financial transactions, the need for strong authentication has drastically increased. Financial institutions in the world are facing a fast approaching deadline to improve user authentication for online banking & other financial institutions. Not only in these fields but the authentication process secures banking, Automatic teller machine (ATM), security entrances, networks, defence forces, top secret projects, personal data of individuals and general websites. Nowadays, most payment services at Point of Sales (POS's) and bank account services at Automatic Teller Machines (ATMs) are protected by a combination of certain unique information stored on a physical device, typically a magnetic stripe card, or a biometric password and PINs. To be successfully authenticated, an adversary has to obtain both the information.

Swipe cards, magnetic cards or electronic chips are most commonly used for authenticating a user in token based authentication systems. But these tokens are very frequently prone to theft and duplication [8]. A common risk of this type of protection is that magnetic stripe cards can be stolen or skimmed by fake card readers. Another important authentication process widely used is using biometric devices. Authentication devices such finger print scanners, voice recognition systems, face-recognition systems are some of the widely used biometric devices. These systems have proven to provide an excellent authentication but with setback's. Biometric devices suffer with list of serious problems. Firstly, they are a costly affair their installation and maintenance also involve lot of money. Secondly, they are very slow when compared to other authentication systems. And thirdly, there are times when it does not accurately recognise the user and asks him to repeat the process again repeatedly. Detailed discussions about biometric authentication and token based authentication are out of the scope of this paper. But once they happen to fail, the security of the authentication scheme relies only on the protection of the PIN.

Personal Identification Numbers (PINs) are widely used in modern information systems to authenticate users. Unfortunately, classical PIN-entry methods are all vulnerable to observation attacks [2, 6]. Moreover by installing key loggers and fake keypads an adversary can easily collect the entire input of a targeted user, from which the adversary can recover the login credentials. Thus, it is possible to obtain login information by shoulder surfing.

What is shoulder surfing?

Shoulder Surfing is using direct observation techniques, such as, looking over someone's shoulder, to get information. Shoulder Surfing is an effective way to get information be it in a user's home while he works on his personal computer or in a public place which is more prone to Shoulder Surfing attack. Shoulder Surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices [1]. The increase in number of laptop and personal digital assistant (PDA) usage has greatly increased the danger of unauthorized observation of authentication procedures. The users have become more prone to password theft due to such kind of sneaking. Especially when the users are moving around it is difficult for them to keep a strict vigilance on their surroundings. One should remain cautious of his/her surroundings if he/she is authenticating by the traditional authentication methods prone to Shoulder Surfing.

In this paper, we propose a new PIN entry scheme, Mirage 1.0. Compared to previous work, this scheme excels in achieving a good balance between security and usability. According to our mathematical analysis, this design can offer a strong security protection against adversaries with both normal cognitive skills and recording techniques using miniature cameras. This scheme is highly interactive and adaptable to all kinds of users irrespective of their age and education. Mirage 1.0 would not only efficiently handle shoulder surfing but would also act firmly against other attacks like key logging, guessing, fake keyboards, and dictionary attacks. With its simple and fast accessible design it depends very less on user's memory and thinking abilities.

The rest of the paper is organized as follows. The related work is reviewed in Section 2. The details of our scheme are presented in Section 3. In section 4 we bring forward a simulation of our model, followed by security analysis in Section 5. In Section 6, we discuss the usability of our scheme. Finally, we conclude our work in Section7.

2. RELATED WORK

Operation Code Authentication [4] is another scheme to overcome shoulder surfing. In this scheme, they have used basic mathematical operations like addition, subtraction, multiplication, and division. They have coded these operations using simple codes. The user at the time of authentication has to recognise these codes and provide a password which is encrypted based on the seeding code dynamically generated on screen. This increases over head over user's both memory and logical skills. Here besides remembering his password, the user also has to remember many other codes. During the time of authentication he also has to encrypt his password himself by doing the calculations given on screen, which is a very inefficient technique. It is a common fact that the more we rely on user's memory and logical abilities the more the system becomes faulty.

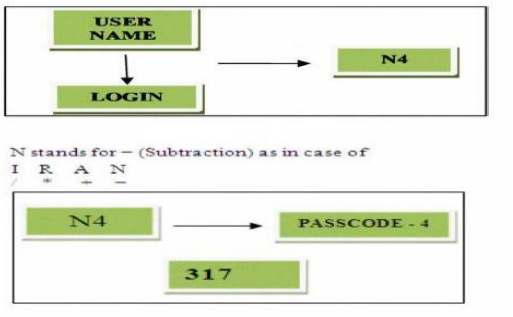

Figure1. Operation code authentication

SS7.0 [1] uses a matrix which contains all characters, numbers. Here in this scheme a user has to enter the row number and column number of the characters of the password. Here the user has to search for characters of his password in the given matrix. This searching is a time consuming job which makes the system more vulnerable to shoulder surfers. The adaptability of the user to this system is also under question.

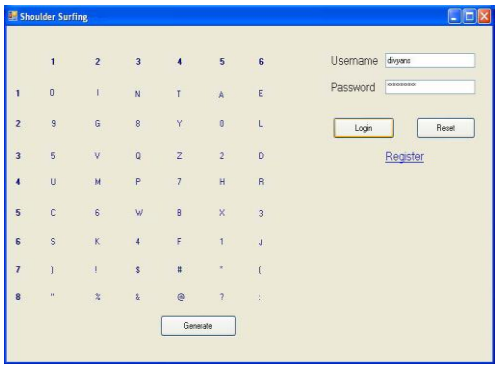

Figure2. A screen shot of SS7.0

The Convex Hull Click Scheme (CHC) is another multiple-round challenge-response authentication scheme proposed to fend off shoulder-surfing. In this scheme, the user needs to select a set of icons, out of a larger number of icons, as their password icons. During the login process, to respond to the challenge, the user must virtually find three or more of his/her password icons, mentally create a convex hull formed by these icons, and then click inside this convex hull. The user must respond to the multiple challenges correctly in order to be authenticated to the system. As a result, the login time can be very long. According to their simulation results, the mean time for correct password inputs is around 72 seconds.

Figure3. Convex hull authentication system

3. PROPOSED SCHEME

Mirage1.0 is primarily a pattern based key entry scheme. Here the user is registered to the system before hand. Like in conventional key entry schemes user has to enter the username and password but what makes it different than the other systems is its password entry scheme. All the process can be divided into two discrete stages, registration and authentication, while in registration phase user has to register himself by giving his username and password. In addition to this user is also to provide pattern in which he would like his password to appear. In authentication phase when user enters his username an interactive screen appears before him. The screen contains a matrix and a password field. Instead of entering the password directly, he has to enter the row and column number of the password character. It is to be noted that password characters would appear only in the pattern in which user has already registered with. This would greatly reduce time taken by the user to search and enter its row and column numbers, reducing the risk of shoulder surfing. For every two entries in password field i.e. row and column number, the matrix refreshes and a whole new matrix appears again. In the matrix appeared there will be repeated characters but user will have to enter the characters only from his registered pattern.

Let us take a example where user has to enter a password "ASTRO". And the following matrix appears on the screen. The highlighting represents the pattern registered by the user which will not be appearing on the original screen

Table 1. Matrix displayed before entering characters

	1	2	3	4	5
1	l	K	f	o	Y
2	R	O	g	*	K
3	3	A	T	S	M
4	a	$	?	i	B
5	e	5	l	q	_

Now the user would enter 32(3rd row, 2nd column element), i.e. 'A'. Now the matrix would get refreshed automatically.

Table 2. Matrix displayed after entering two characters

	1	2	3	4	5
1	&	K	p	9	S
2	A	S	g	*	a
3	3	R	O	T	j
4	g	M	r	b	Z
5	/	5	0	S	_

Now the user would be expected to enter 22(2nd row, 2nd column element), i.e. 'S'. If you notice it is seen that there more than one 'S' in the matrix, but the user would be expected to enter only the one from his chosen pattern. As usual the matrix refreshes again.

Table 3. Matrix displayed after next two characters

	1	2	3	4	5
1	6	U	f	o	E
2	O	T	h	(	k
3	7	R	A	S	n
4	q	^	@	f	d
5	o	5	l	q	-

Now the user would be expected to enter 22(2nd row, 2nd column element), i.e. 'T'. If you notice then you would certainly find that entry made this time and before the matrix got refreshed is same. This would enhance its capabilities to evade shoulder surfing.

Table 4. Matrix displayed after next two characters

	1	2	3	4	5
1	l	t	&	s	Y
2	A	T	G	%	R
3	3	S	O	R	M
4	*	$	@	A	R
5	A	R	O	Q	-

Now the user would be expected to enter 34(3rd row, 4th column element), i.e. 'R'. And the matrix refreshes again.

Table 5. Matrix displayed after next two characters

	1	2	3	4	5
1	L	4	F	J	s
2	A	O	)	t	L
3	*	S	T	R	M
4	X	s	?	L	#
5	A	$	O	Q	u

Finally the user would be expected to enter 22(2nd row, 2nd column element), i.e. 'O'. Hence instead of entering the original password, ASTRO, the user enters '3222223422'.

4. SIMULATION

A detailed stepwise simulation of Mirage 1.0 is shown below. As said earlier the whole process could broadly divided into two parts.

4.1 Registration

Initially user has to register himself in order enjoy the facilities of this system. Registration involves registration of user details and user desired pattern.

Figure4. A screen shot of user registration of Mirage1.0

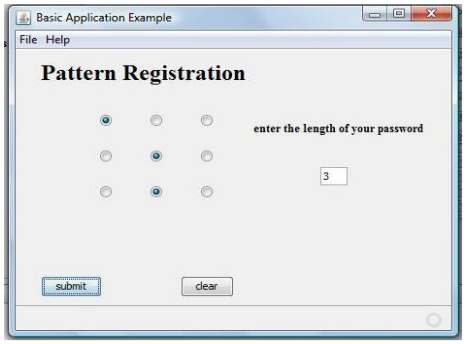

Figure5. A screen shot of pattern registration of Mirage1.0

After entering the entire details user has to select a pattern which is to be used later while authentication. The above figure shows pattern registration for passwords with length 3.

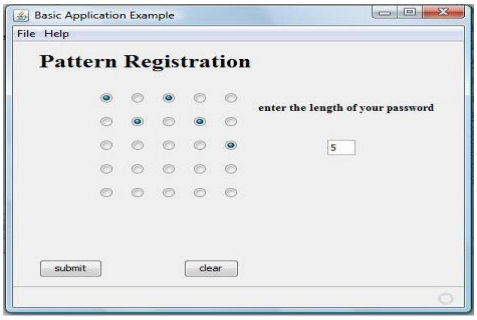

Figure6. A screen shot of pattern registration of Mirage1.0

The above screen shot is pattern registration for password length 5.

4.2 Authentication

In order to logon a user initially requires authenticating himself/herself by providing user name and password. There will be two fields: one containing user name & the other containing password. The user name is entered, as usual. While entering the password, a new scheme is being applied. As it is evident from Figure.7, a randomized matrix of alphanumeric characters and symbols is present. The user has to find out the corresponding position of his/her password and provide the positions as his/her password in the password field (excepting for the last three elements of the password which the user enters as usual). Then 'Submit' is clicked for verification of the correctness of the provided username & password.

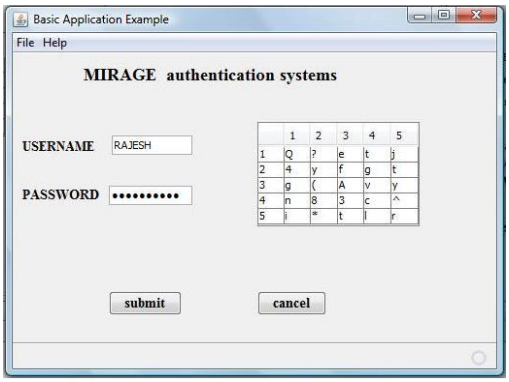

Figure7. A screen shot of user authentication in Mirage1.0

If the authentication fails then an error message is generated asking the user to retry.

Figure8. A screen shot of error message in Mirage1.0

5. USABILITY

Mirage 1.0 takes the process of safe login to whole new next level. Mirage due its simple and robust design can be one of the best solutions for countering shoulder-surfing. Our scheme can effectively stop both cognitive and recording based shoulder-surfing. We have further improved its efficiency by including RSA encryption in the scheme. The encryption and decryption process is carried out automatically without the user's involvement. Thus, the sending of the password to a remote database to check for its correctness particularly in a networked environment will not cause any problem. The havoc of loss of passwords through illegal tapping of messages during its transportation can be eliminated through this. Furthermore this scheme is totally immune to different other attacks like fake keyboards, dictionary attacks and key logging. Because the design is simple to use, users need not be trained. Our design uses textual information and representations only, hence reducing the unnecessary usage of memory like in other graphical key entering schemes. User's of this system do not need any special skills and also do not need remember many codes.

From the above discussion it is evident that our proposed scheme (Mirage 1.0) is a very effective solution for controlling and eliminating shoulder surfing.

6. SECURITY ANALYSIS

In this section, we analyze the security of our scheme under three types of Shoulder-Surfing models, i.e., guessing attacks, recording based shoulder-surfing (RSS) and cognitive shoulder surfing (CSS).

6.1. Guessing attacks

Under this model, the adversary knows nothing about the secret PIN, and thus can only launch a random guessing attack.

Let us say Pr be the probability of an adversary making a successful login. Let N denote the number of pin combinations achieved by using the matrix being displayed and A be the number of successful combinations from N. Hence the probability of getting a successful login by an adversary would be

$$Pr=A/N$$

For a 3 character password, since the order of matrix would be 3X3, the N value should be 504(9*8*7). Hence Pr=1/504, only a 0.001% probability of successful login.

Similarly, for a 4 character password it would be, Pr=1/3360, far less than the previous one. It could be further decreased by using higher password lengths.

6.2. Recording based shoulder surfing

By using a miniature camera or some kind of recording device the adversary might be able to know the characters of the password entered by the user [10]. In our scheme we have added similar looking or same duplicate characters like the original characters. But unless the adversary knows the pattern he cannot justify which characters is the actual password character.

In our scheme every password character would at least have 2 duplicates. Keeping this in mind we design a probability function Pr.

Let us say if the password length is 3 there will be minimum of 6 pairs of similar characters. Then N would be 120(6*5*4) and the probability would be

$$Pr=1/120,$$

This shows that just by using password of 3 characters, we can prevent recording based shoulder surfing to about 99.1%.

6.3. Cognitive shoulder surfing

There has been some interesting research on the cognitive capabilities of human beings. In 1956, Miller [11] noted that the limitation on short term memory (STM) is 7 plus or minus 2 symbols. A more recent work by Vogel *et al.* [11] shows that STM of normal people is limited to three to four symbols. Few subjects were able to remember five symbols in their STM throughout the experiments conducted in [11]. This discovery is based on the neurophysiologic evidence. Since the matrix in our model keeps refreshing for every entry, it is highly difficult for a person with normal cognitive skills to shoulder surf on this system. More over a single person can never notice both keyboard and screen simultaneously. Thus the proposed scheme is resilient to cognitive shoulder surfing.

In addition to these we have embedded our system with RSA security algorithm to prevent eavesdropping over networks and dictionary attacks.

Table 6. The following table shows a comparative study of different existing authentication systems with our proposed scheme

S.No	Key entry scheme	Ability to stop cognitive shoulder surfing	Ability to stop recording based shoulder surfing	Adaptability	Ease of use	Resilience against other attacks
1	Operation code authentication.	It can safeguard user from this attack but with limitations	It cannot help user if the whole login process is being recorded	It would take many logins for a user to become comfortable.	Very difficult for a person with average logical skills	It does not provide any encryption mechanisms and vulnerable to guessing attacks.
2	SS7.0	It can prevent attacks made by a person with average cognitive skills	It is cannot prevent this type of attack	Adaptable only after some initial training	User has to search for his password characters.	It is resilient towards some attacks like key logging
3	Convex hull	It can prevent these type of attacks	It is vulnerable if someone records many logins.	Adaptable only after some initial training	User has to search for the items	It does not provide any other resilience.
4	Pass face	It can prevent attacks made by a person with average cognitive skills	It is cannot prevent this type of attack	It needs lots of system memory for storing many pictures.	User has to memorize many faces.	It does not provide any other resilience.
5	Déjà vu	It can prevent attacks made by a person with average cognitive skills	It can not prevent it if many logins have been recorded	It needs lots of system resources for generating graphics	Very high chances of getting confusion	It does not provide any other resilience.
6	MIRAGE 1.0	It can prevent this attack even if the attacker has excellent cognitive skills	It can prevent such attacks even though many logins are recorded	With a interactive screen provided it is very adaptable with just few minutes of training.	Very easy to find password characters because user already knows the pattern	It is equipped with RSA encryption algorithm and is safe against attacks like guessing and key logging.

7. CONCLUSION

Password theft is now a major security concern. Unfortunately there are no efficient schemes developed to regulate this crime. In this paper we have proposed a novel technique which uses patterns to authenticate users. We have proposed a scheme that would handle any kind of password theft. First, we have elucidated the proposed scheme with relevant examples. When compared to existing solutions, our scheme, Mirage1.0 is more effective and reliable. It's simple and robust design makes it easy to implement and adapt. Secondly, we have discussed how well this scheme can handle different thefts like shoulder surfing, dictionary attacks, fake keypads and other ways. We have further strengthened our model by a detailed mathematical analysis.

8. REFERENCES

[1] Divyans Mahansaria, Samarpan Shyam, Anup Samuel, Ravi Teja, Massachusetts Institute of Technology. "A fast and secure software solution [SS7.0] that counters shoulder surfing attack". Proceedings of 13thIASTED International conference software engineering and application (SEA 2009), November 2-4,2009, Cambridge, MA, USA.

[2] M. Brader. Shoulder-surfing automated. Risks Digest, 19, 1998.

[3] G. A. Miller. The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review, 63:81–97, 1956.

[4] Shabih ul Hasan Naqvi, S. Afzal, S. "Operation code authentication". Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference .9th july,2010.

[5] V. Roth, K. Richter, and R. Freidinger. A pin-entry method resilient against shoulder surfing. In Proc. of 11th ACM Conference on Computer and Communication Security (CCS 2004), pages 236–245,Washington DC, USA, October 2004. ACM Press.

[6] C. Summers and S. Toyne. Gangs preying on cash machines.BBC NEWS Online, Oct. 2003.

[7] D.Weinshall. Cognitive authentication schemes safe against spyware (short paper). In Proc. of the 2006 IEEE Symposium on Security and Privacy (S&P 2006), pages 295–300, Berkeley/Oakland, California, USA, May 2006. IEEE Computer Society.

[8] ATMScam. Bank ATMs converted to steal bank customer ids. http://www.utexas.edu/police/alerts/atm scam/.

[8] M. Brader. Shoulder-surfing automated. Risks Digest, 19, 1998.

[9] V. Roth, K. Richter, and R. Freidinger. A pin-entry method resilient against shoulder surfing. In Proc. Of 11th ACM Conference on Computer and Communication Security (CCS 2004), pages 236–245,Washington DC, USA, October 2004. ACM Press.

[10] P. Shi, B. Zhu, and A. Youssef. A new pin entry scheme against recording-based shoulder-surfing. InProc. of 3rd International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009), Athens/Vouliagmeni, Greece, June 2009. IEEE Computer Society.

[11] E. K. Vogel and M. G. Machizawa. Neural activity predicts individual differences in visual working memory capacity. Nature, 428:748–751, April 2004.

[12] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proc. of the working conference on Advanced visual interfaces (AVI 2006), pages 177–184, Venezia, Italy, May 2006. ACM Press.

[13] Peipei Shi, Bo Zhu and Amr Youssef. Concordia Institute for Information Systems Engineering. "A Rotary PIN Entry Scheme Resilient to Shoulder-Surfing.". Internet Technology and Secured Transactions, 2009. ICITST 2009.

[14] T. Perkovic´, M. C˘ agalj, N. Rakic´. Dept. of Electrical Engineering, FESB, University of Split. "SSSL: Shoulder Surfing Safe Login". Software, Telecommunications & Computer Networks, 2009. SoftCOM 2009. 17th International Conference,26 sept,2009.