Cryptanalysis of a Shoulder-Surfng Resistant Password Authentication Scheme

Maw-Jinn Tsaur
Department of Information Technology
Tungnan University
New Taipei, Taiwan, R.O.C.
e-mail: mjtsao68@gmail.com

Chung-Chia Lue
Department of Information Technology
Tungnan University
New Taipei, Taiwan, R.O.C.
e-mail: cclu@mail.tnu.edu.tw

***Abstract*—Researchers have been trying to improve authentication for a long time. User still uses textual passwords to authenticate the systems. However, since weak textual passwords are susceptible to the dictionary attack and strong textual passwords are hard to remember. Graphical passwords have been proposed as an alternative to textual passwords because graphical passwords can increase password memorability. However, most textual and graphical passwords are vulnerable to shoulder-surfing attacks. Shoulder-surfing attacks refer to using direct observation techniques, such as looking over someone's shoulder, to get password. Shoulder-surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. In 2011, C. Srinadhu etc. proposed a textual password scheme, MIRAGE 1.0 scheme, to reduce shoulder-surfing attacks. This paper reviews MIRAGE 1.0 scheme and discusses its advantages and disadvantages.**

Keywords-weak textual passwords; strong textual passwords; graphical passwords; shoulder-surfing attacks

I. INTRODUCTION

Nowadays, wider usage of networks makes the life more convenient. However, in the mean while, more and more attacks are happening in the network to endanger network security. Password authentication is regarded as one of the simplest and most convenient authentication mechanisms. Existing one-time password authentication schemes can be categorized into two types, one requires only weak texture passwords and the other must use strong texture passwords. However, since weak texture passwords are susceptible to the dictionary attack and strong texture passwords are hard to remember. Graphical passwords have been proposed as an alternative to textual passwords because graphical passwords can increase password memorability[9][10]. However, most textual and graphical passwords are vulnerable to shoulder-surfing attacks [1][2][3]. Shoulder-surfing attacks refer to using direct observation techniques, such as looking over someone's shoulder, to get password[6][7]. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. In 2011, C. Srinadhu etc. proposed a textual password scheme, MIRAGE 1.0 scheme, to reduce shoulder-surfing attacks [4]. In this paper, we show that the MIRAGE 1.0 scheme is still vulnerable to a serious shoulder-surfing attack.

The sequel is organized as follows. Section 2 we will review MIRAGE 1.0 scheme. Section 3 we will analyze security of MIRAGE 1.0 scheme. Finally, a conclusion is given in section 4.

II. REVIEW OF MIRAGE 1.0 SCHEME

The notation used throughout this paper is described as follows.

- *U* denotes the user.
- *S* denotes the system.
- *n* denotes the total number of characters in a challenge.
- *R* denotes the total number of rounds chosen by S.

Registration Phase

This phase is only invoked once when *U* registers to *S*. The system firstly displays the registration screen. Then *U* enters name, username, and password. *U* and *S* have to remember the username and password and keep them confidential. *U* enters name, username, and password through a secure environment. Fig. 1 shows an example with a registration screen for MIRAGE 1.0 scheme.

Figure 1. An example with a registration screen for MIRAGE 1.0 scheme

In addition to entering password, user also has to provide a pattern that he would like his password to appear. Fig. 2 shows an example with a pattern for MIRAGE 1.0 scheme.

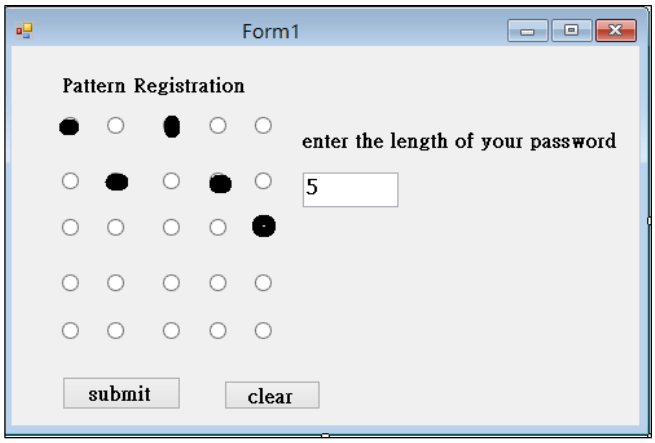

Figure 2. an example with a pattern for MIRAGE 1.0 scheme

Login Phase

This phase is only invoked whenever *U* requests to login *S*. At first, *n* are randomly arranged in the password challenge window. These characters include mostly non-password characters along with a few password characters. Instead of entering a password character directly, *U* has to enter the row and column number of the password character. The login phase involves *R* challenge-response rounds. Once *U* has entered one password character, *n* are randomly arranged in the password challenge window. If *U* sequentially enters the password characters from his registered pattern, then *S* authenticates *U*. Otherwise, *S* rejects *U*'s login request and terminates this session. Fig 3 ~ Fig. 7 shows a successfully login example for MIRAGE 1.0 scheme. The login password is "ASTRO"

	1	2	3	4	5
1	R	S	O	T	O
2	1	A	h	T	m
3	M	N	J	Y	S
4	L	P	0	e	c
5	A	F	f	s	g

Figure 3. Entering 22 for "A" password character

	1	2	3	4	5
1	A	g	R	*	a
2	0	S	4	O	7
3	3	j	a	b	T
4	&	k	p	9	s
5	/	5	0	s	

Figure 4. Entering 22 for "S" password character

	1	2	3	4	5
1	O	h	T	c	k
2	0	R	4	A	7
3	3	j	T	b	S
4	q	^	@	f	d
5	o	s	1	q	9

Figure 5. Entering 13 for "T" password character

	1	2	3	4	5
1	A	G	T	%	R
2	4	S	7	O	j
3	*	$	A	k	R
4	l	t	&	s	y
5	A	R	O	Q	5

Figure 6. Entering 35 for "R" password character

	1	2	3	4	5
1	A	*	O	M	O
2	4	S	6	T	k
3	)	t	L	9	R
4	L	4	F	J	S
5	X	s	?	L	#

Figure 7. Entering 13 for "O" password character

III. SECURITY ANALYSIS OF MIRAGE 1.0 SYSTEM

A keylogger, sometimes called a keystroke logger, key logger, or system monitor, is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard [5]. A general shoulder-surfing attacker observes each one enters on the screen from the user. A serious shoulder-surfing attacker records one entering on the screen from the user through hidden-camera and a keylogger. We found that MIRAGE 1.0 scheme can resist the keylogger attack and the general shoulder-surfing attack, but it cannot resist serious the shoulder-surfing attack.

A. Keylogger attack

In MIRAGE 1.0 scheme, user enters password characters are different every time with the same password and a attacker will capture different password characters each time using a keylogger, therefore it can resist the keylogger attack.

B. General Shoulder-sufing attack

In 2011, Srinadhu et al. claimed that MIRAGE 1.0 scheme can reduce shoulder-surfing attack [4]. We found that MIRAGE 1.0 scheme offers perfect resistance to general shoulder-surfing attack because there are many same characters with the correct password in the password

challenge window; the attacker cannot know which character is the correct one. This shows that the general shoulder-surfing attack to MIRAGE 1.0 scheme is physically infeasible.

C. *Serious Shoulder-sufing attack*

In MIRAGE 1.0 scheme, an attacker first can get the pattern of user's passwords through a keylogger. Then he can get the characters that user's entered through hidden-camera[8]. Finally, he can gain the correct information of user's password. This shows that the serious shoulder-surfing attack to MIRAGE 1.0 scheme is physically feasible.

IV. CONCLUSION

We have reviewed MIRAGE 1.0 scheme. We also analyzed MIRAGE 1.0 scheme and found that MIRAGE 1.0 scheme can withstand the keylogger attack and the general shoulder-surfing attack, but it cannot withstand the serious shoulder-surfing attack. Our future work will propose some solutions to the serious shoulder-surfing attack.

REFERENCES

[1] A. Forget, and S. Chiasson, and R. L Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," Proceedings of the 28th international conference on Human factors in computing systems, 2010.

[2] P. Shi, B. Zhu, and A. Youssef., "A new pin entry scheme against recording-based shoulder-surfing," In Proc. of 3rd International Conference on Emerging Security Information, Systems and Technologies, 2009.

[3] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," In SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security, 2007.

[4] C. Srinadhu, S. K. Addanki, and B. R. Acharyulu, "MIRAGE 1.0: A Key Entry Scheme Resilient to Shoulder Surfing," International Journal of Computer Applications, 0975-8887, Vol. 19-No1, Sep. 2011.

[5] M. Rouse, "keylogger (keystroke logger, key logger, or systemmonitor), " Article in http:// searchmidmarkets ecurity.techtarget.com /definition/keylogger.

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

[7] C. Summers and S. Toyne. Gangs, "preying on cashmachines, " BBC NEWS Online, Oct. 2003.

[8] D. Mahansaria, S. Shyam, A. Samuel, Ravi Teja, "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.

[9] S. Madigan, "Picture memory," Imagery, Memory and Cognition, pp. 65–89, 1983.

[10] S. Madigan and V. Lawrence, "Factors Affecting Item Recovery and Hypermnesia in Free Recall," American Journal of Psychology, vol93,pp.489-504,1980.