A Password Authentication Method Tolerant to Video-recording Attacks analyzing Multiple Authentication Operations

Yutaka Hirakawa, Yutaro Kogure, and Kazuo Ohzeki

Abstract**—**User authentication is widely used in Internet services, such as Internet banking, Internet shopping, and Internet finance. In authentication, ID and personal identification number (PIN) or textual passwords are commonly used. There is a risk to be captured these secure information through shoulder-surfing or by the use of concealed miniature cameras. This article discusses a means of improving a user authentication method that accepts textual passwords and that is tolerant to observation attacks. A vicious observation attack, or a video-recording attack, where the user's password selection operation is video recorded, is well known. Conventionally, a few methods are tolerant when password selection operations are video recorded two times. However, the conventional methods are not tolerant when authentication operations are video recorded more than two times. This article proposes a user authentication method that is tolerant to attacks when the user's authentication operations are video recorded more than two times.

Keywords**—**password authentication method, video-recording attack, security

I. Introduction

INTERNET is widely used and is a part of infrastructure of our society. User utilizes many kinds of internet services, such as Internet shopping, Internet banking, and Internet finance, every day. In these Internet services, user authentication is widely used. There is a risk to be captured these secure information through shoulder-surfing or by the use of concealed miniature cameras. If the ID and passwords for the internet services are leaked, it leads to enormous damages.

Currently, conventional text passwords are commonly used for user authentication. This article discusses text password authentication method. Nowadays, each user uses variety kinds of devices, such as personal computers, tablet computers, and smart phones. The text password method is considered to have an advantage because it is easy to offer suitable interface to variety of devices without additional equipment.

Recently, there are huge amount of small cameras in our society. Almost every one has a mobile phone or smart phone with camera function. A large number of monitor cameras are settled at many places in every town and every office. If authentication operation is video recorded, the ID and password are easily stolen.

As an example of crisis using video cameras, an ATM password was stolen with the aid of a wireless charge-coupled device (CCD) camera recording in Japan in October 2005. The perpetrators had set up many cameras at various ATMs in Tokyo. The bank's investigation revealed that user operation was captured by hidden cameras at more than 60 ATMs in the metropolitan area [1, 2]. Whenever a similar crisis occurs, it is not surprise.

Biometric authentication technology is a possible solution [3, 4] to this problem. However, because users use variety kinds of devices and the aforementioned solutions require additional equipment; the problem is a current concern.

In this article, we use a term "video recording attacks". It means that malicious persons record authentication operations and analyze video to narrow down the numbers of password candidates. If malicious persons get videos recorded by monitoring cameras in some companies, the video may include a certain persons operations in a certain periods. In such case, malicious person can analyze a certain user's multiple authentication operations and may capture his passwords.

There are a few methods[5,6] those are tolerant to shoulder surfing or observation attacks. However, the most of all methods are not tolerant to video recording attack using recorded video analysis. If some methods are tolerant to recording video analysis of one time authentication operations, which means authentication operations on someday, the most of the methods are not tolerant to video recording attack by analyzing plural authentication operations, which means plural authentication operation on Monday and Wednesday.

Conventionally, there are a few methods that are tolerant when a user's authentication operations are video recorded twice. But there is no report of password authentication method tolerant to video-recording attacks analysing more than two different authentication operations of the same person.

This article proposes a text password authentication method that uses numeric or alpha-numeric passwords and is tolerant when a user's authentication operations are video-recorded more than two times.

The remainder of this article is organized as follows: Section II reviews related works. Section III discusses existing two techniques which seem to be tolerant to video-recording attack analyzing multiple authentication operations. But, through an experiment, the way to narrow down the number of password candidates by the analysis of multiple authentication operations

Yutaka Hirakawa is with Shibaura Institute of Technology, Tokyo 135-8548, Japan. (phone:+81-3-5859-8509; e-mail:hirakawa@shibaura-it.ac.jp)

Yutaro Kogure is with Shibaura Institute of Technology, Tokyo 135-8548, Japan. (e-mail: al11040@shibaura-it.ac.jp).

Kazuo Ohzeki is with Shibaura Institute of Technology, Tokyo 135-8548, Japan. (e-mail: ohzeki@sic.shibaura-it.ac.jp)

is described. Section IV proposes an authentication method which is tolerant to video-recording attacks analyzing multiple authentication operations, and its usability evaluation is shown. Section V summarizes the article.

II. Related work

Various studies on authentication methods that use textual passwords have discussed observation attacks [5 -15].

In [5], a password authentication technique called PIN-entry using numeric key entry is proposed. On the display, a white or black background is randomly shown. A user does not designate a password, but selects white or black as the password's background color. For password entry for each digit, the user designates the background color from a different color pattern four times. This method is safe against shoulder surfing; however, if the input operation is video recorded, the password can be discovered easily.

In [6], an interface for textual passwords, S3PAS, is proposed. Many characters are displayed on the interface. A user designates three points where a pass-character is included in a triangle. This method is also safe against shoulder surfing; however, if the input operation is video recorded, the password can be discovered easily.

In [7, 8], an authentication method using numeric key entry called FakePointer is proposed. In this method, a disposable "answer selection information" must be retrieved before each authentication. This information specifies a background mark such as a diamond, square, circle, or octagon for the displayed numeric password. For authentication, the user presses the "Enter" button, which adjusts the password according to the background mark. If the answer selection information is safely retrieved before each authentication, it is tolerant when a user's password selection operation is video-recorded two times. However, studies do not discuss the safe retrieval of the answer selection information.

A textual password entry interface called mobile authentication is proposed in [9, 10]. In this method, the selectable texts are arranged in a square. Each text has a background color. Each password is alphanumeric, and the texts are arranged in a 10 × 5 square using 10 background colors. Each background color appears only once in each row. The color pattern of a row is the permutated color pattern of another row. In this method, a password is divided into multiple short passwords. For example, an 8-length password consists of two 4-length passwords. The user must register the password division pattern, e.g., 4-length and 4-length for the 8-length password, beforehand. In the authentication operation, the user selects the same color for each short password. For example, a red background is used for the former 4-length password, and a green background is used for the latter 4-length password. The color is freely determined by the user for each authentication operation. Although this technique has the restriction that all available texts must be displayed on the authentication interface, it is secure when a user's password selection operation is video-recorded two times. But it is not tolerant to video recording attack analyzing videos authentication operation recorded more than two times.

In [11 - 13], authentication methods using random selection and ambiguity introduction to keep tolerance to video recording attacks are proposed. But methods are tolerant to video recording attacks analyzing only equal or less than two times authentication operations.

III. Conventional methods seem to be torelant to multiple video recording attacks

This section discusses two conventional methods [14, 15] which seem to be tolerant to video-recording attacks analyzing multiple authentication operations. Outlines of these methods are described, and experimental authentication results are shown. At last, it is shown that the number of password candidates can be narrow down by analyzing recorded video of authentication operations.

A. Pass-number authentication method using voice navigation[14]

This is a PIN (Personal Identification Number) code authentication using numerical password. At first, the system designates an arbitrary number by voice announcements. Then a user modifies the designated value to the correct numeric password value by increase or decrease operations. For example, "3" is designated by voice announcement for the first pass-number. Assume that the password is "5628", and the correct first pass-number is "5". Then a user operates increase operation twice (designated number:3 + 2 = password:5) and push the enter button. The similar operation is repeated as same times as the length of numeric password.

This method seems to be tolerant to video recording attacks. The proposed method assumes a smart phone use. For the increase operation, a user's action is an upwards flick, touch display by a finger and move to upwards. Similarly, decrease operation is a downwards flick. Nowadays, many people bring his own ear phone and use his smart phone or mobile phone as an mp3 player. So voice announcements adoption to avoid observation attacks seems to be realistic.

This method claims the method is tolerant to shoulder surfing or video recording attacks.

B. Pass- number authentication method using vibration[15]

This method is also a numerical password authentication. The frame work of this method is similar with the method described in 3.1. A different point is a vibration use instead of voice announcement. This method offers an operation interface shown in Fig. 1. In the explanation, we use a word "place". In authentication, the system designates a "place", and a user moves a correct numeric password to the designated place. When a user starts authentication, the system offers arbitrary number of vibration. If short vibration is repeated 5 times, it means that the target "place" is 5. Then a user moves correct numeric password under the place of P5 in the upper line in Fig. 1.

It may be doubtful that the number of vibration is easily recognizable. Moreover, a person may notice vibrations of neighborhood's smart phone. It needs more detailed discussions. Anyway, the method itself seems to be tolerant to video-recording attacks analyzing multiple authentication

operations.

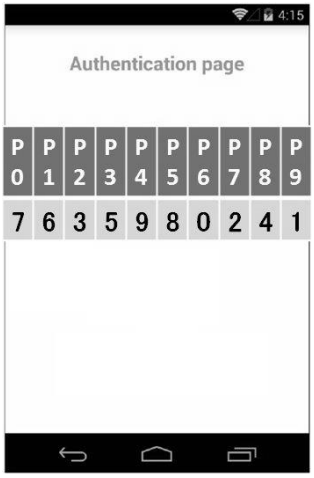

Fig. 1 Authentication Interface[15]

C. Password estimation experiment

In this subsection, through an authentication experiment we try to prove the following hypothesis.

[Hypothesis] It is possible to narrow down password candidates by analyzing partiality of human's operation.

The experimental interface is shown in Fig. 2. It is helpful to compare Fig.2 with Fig. 1. Fig. 2 indicates that the correct authentication operation is a move of numeric password to the place under "place" 7, assuming a correct numeric password is currently placed on the place of star symbol. Using this interface, one numeric password authentication is repeated 700 times. Experimental cooperators are 14 students. In each experiment, the position of star is randomly selected.

Fig. 2 Experiment system display

A part of experimental results is shown in Fig. 3. Fig. 3 is a summary data useful for malicious person. If authentication interface is displayed as shown in Fig. 2, possible operations are two operations, such as move right 7 times or move left 3 times, where the left from the left end is defined the right end, and the right of the right end is defined the left end. Fig. 3(1) shows that there are 3 persons who select 7 right moves when password character places on position 0 and the target place is position 7. Otherwise, another 6 persons select 3 left moves in the same occasion. These two operation candidates also appears when the star symbol is under "1" and a message is "plase move star symbol under place "8"", and other 8 cases. Fig. 3(1) is a summary of those.

position of ★ (password)	target place	3 * left move operation	7 * right move operation
0	7	6	3
1	8	3	5
2	9	3	6
3	0	8	0
4	1	11	0
5	2	4	0
6	3	4	0
7	4	10	0
8	5	9	0
9	6	9	0

(1) 3 left move shortest case

position of ★ (password)	target place	5 * left move operation	7 * right move operation
0	5	0	3
1	6	0	7
2	7	0	8
3	8	0	9
4	9	0	10
5	0	7	0
6	1	10	0
7	2	5	0
8	3	7	1
9	4	6	0

(2) 5 left or 5 right move shortest case

Fig. 3 Experiment results (a part)

It is interesting that the right move 7 times only appears in upper 3 rows. The first row indicates that a user moves star symbol placed under "0" to place "7" by 7 right move operations or 3 left move operations. But, the fourth row indicates that all user move star symbol under "3" to place "0" by 3 left move operations. There is no person to move star symbol under "3" to place "0" by 7 right move operations. In the cases of fourth row to tenth row, distance of required move is three. So every user operates along obvious shortest path. But, in the cases of upper three rows, many people move along long distance. A user may not aware that the shortest path is left move, and selects 7 right moves which are considered to be intuitive operations.

Through the discussion in the above, it is very important that malicious persons estimate the correct password does not place under the place from "3" to "9", if a user chooses 7 right move operations. This information is very useful to narrow down password candidates for malicious persons.

On the other hand, Fig.3(2) shows a results of the case that 5 left move or 5 right move is the shortest operation. There is one exception, but when a malicious person observes 5 right move or left move operation, he can narrow down password candidates from 10 to 5.

Using the data of above experiment, the narrow-down process of the number of password candidates is simulated. We assume the password length is four and a correct password is arbitrary selected. If there is no useful estimation, the number of candidates is 10000. By our simulation, the number of password candidates becomes under 1000 by average 6.1 times analysis of recorded videos. Also, the number of password candidates becomes fewer than 100 by average 42.6 times analysis of recording videos.

The important point is the existence of the worst case. In the worst case, each pass-text has very small ambiguity, only three candidates by the video analysis of an authentication operation. Therefore, only 81 password candidates for 4-length password, and 729 password candidates for 6-length password by video analysis of one time authentication operation.

In the experimental interface, there is no panel of password numeric. If password panels are displayed in random order in the same manner with Fig. 1, the worst case becomes more serious. In the worst case, candidates of each pass-text may be narrow down to only three candidates in the first authentication operation analysis, and the correct pass-text may be found out in the second authentication operation analysis. Thus, there is danger by which all passwords may be found out through the

analysis of video recorded two times authentication operations.

Thus it is proved that the above hypothesis holds.

IV. Proposed Authentication Method

In the previous section, it is shown that the number of password candidates can be narrowed down by analyzing authentication operation videos. This section proposes a revised method.

A. revised authentication method

We propose the authentication method which is tolerant to video-recording attacks analyzing multiple authentication operations. We assume textual passwords which are constructed with numeric or alpha-numeric. The proposed authentication adopts voice guidance in the similar manner as the conventional authentication method explained in the previous section. The authentication interface is shown in Fig. 4.

In authentication operations, for each pass-character, voice guidance designates a target place where the correct password must be placed by a user's operation. The similar operation are repeated as same times as the length of passwords. As shown in Fig. 4, the correct pass-text should be moved by a user inside the designated place by voice guidance.

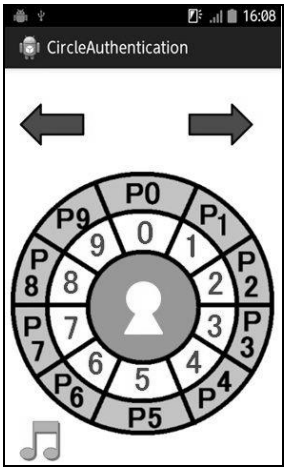

Fig. 4 Proposed Authentication Interface

In the conventional method, panels are placed on a line, where the right position of the right end panel is the left end panel. This uncontinuity is the cause of the distribution partiality in human operations. And it brings weakness in authentications. On the other hand, panels are lined circularly in the proposed method. For every pass-number move operation, there is no useful information to narrow down the number of password candidates.

It is considered to be important that there is no worst case in the proposed method. Because there is no useful information to narrow down the number of password candidates. Thus, it is tolerant not only from the average probability viewpoint, but also from the viewpoint of worst case evaluation.

B. Usability evaluation

The conventional method is shown to be not tolerant to video-recording attack analyzing multiple authentication operations in the previous section. The proposed method solves the problem and achieves high tolerance. In this section, it is verified whether there is any compensation in usability.

The authentication interface used in this evaluation is shown in Fig. 4. In the outer circle, there are 10 position panels, one of which is designated by voice announcement. In the inner circle, there are 10 numeric panels. When voice announcement designates "position" 0 and correct numeric pass-text is 9, a user touches right arrow icon once and touches the center key hole to enter password and refresh display for the next authentication operation. The music note icon is for repeating the voice announcement. Numeric panels are in random order in conventional method [11]. But increasing order layout is adopted in the evaluation. Because it does not affect to tolerance, and the increasing order layout is more intuitive for users.

In the evaluation, beside of conventional method, an authentication interface using alpha-numeric password is also added to evaluation target. Its authentication interface is shown in Fig. 5. For alpha-numeric password, position panels are layout in an outer circle, which is not moved. To touch right arrow, inner two circles move clockwise. When password is "z" and voice announcement designate "P2" as the target place, the correct operation is 2 times right arrow touch. In this interface, when the correct password is "y", authentication is also 2 times right move. It includes ambiguity. But the system can correctly decide the validity of user's authentication operations.

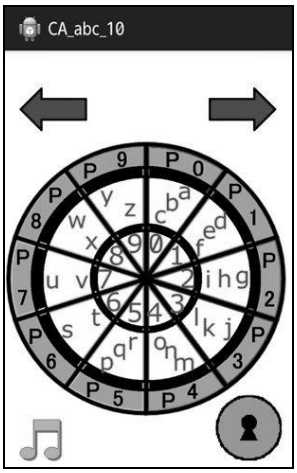

Fig. 5 Interface for alpha-numeric password

The results of usability evaluation are shown in Fig. 5. The first one is for conventional authentication method with 4-length numeric password. The second one is for proposed authentication method with 4-length numeric password. The last one is for proposed authentication method with 6-length alpha-numeric password, whose interface is shown in Fig. 6. In each method, it takes about 4 second for one pass-character authentication. There is no significant difference among three operation times and error rates. Thus, it is verified that strong tolerance is realized without paying any compensation in usability.

	time for authentication	error rate
conventional method	23.3 sec (4 length)	0.03
proposed method (numeric pass)	22.3 sec (4 length)	0.03
proposed method (alpha-numeric pass)	30.19 sec (6 length)	0.03

Fig. 6 Usability evaluation results

V. Conclusion

This article proposes a user authentication method that uses passwords consisting of text characters. Conventional methods are tolerant to video recording attacks which records authentication operations equal or less than two times. However, the proposed authentication method is tolerant to video recording attacks even if multiple authentication operations are video recorded. Moreover, the method is tolerant not only from the average probability view point, but also from the worst case evaluation.

Any conventional authentication method using textual password is not tolerant against video recording attacks if multiple authentication operations are video recorded. The proposed method can be used on variety kinds of devices, such that desktop PCs, notebook PCs, tablet PCs, and smart phones without any additional equipment.

References

[1] The Mitsubishi Tokyo UFJ bank, 'A bank report about that the camera was put on secretly at the ATM machine by some person'. http://www.bk.mufg.jp/info/ufj/ufj_20051101.html

[2] Bank of Yokohama, 'A bank report about that equipment for the sneak shot was installed in the unmanned agency (the ATM out of the store)'. http://www.boy.co.jp/info/pdf/9.pdf

[3] M. Une, T. Matsumoto, 'About the fragilitas about the living body authentication: It studies mainly a fragilitas about the counterfeiting of a stigma by the finance', Monetary Research, vol. 24, no. 2, pp. 35-84 (2005)

[4] Banno, 'The recent trend, the forensic science technology of the living body authentication technology', International Journal of Information Technologiy and Computer Science, vol. 12, no. 1, pp. 1-12 (2007)

[5] V. Roth, K. Richter, R. Freidinger, 'A PIN-entry method resilient against shoulder surfing', CCS'04, pp. 236-245 (Oct 2004)

[6] H. Zhao, X. Li, 'S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme', IEEE Advanced Information Networking and Applications Workshops 2007, pp. 467-472 (2007)

[7] T. Takada, 'FakePointer: The authentication technique which has tolerance to video recording attacks', IPSJ Transaction, vol.49, no.9, pp.3051-3061 (Sep 2008)

[8] T. Takada, 'FakePointer2: The proposal of the user interface to improve safety to the peep attack about the individual authentication', Cryptography and Information Security Symposium, SCIS2007 (2007)

[9] S. Sakurai, M. Yoshida, T. Munaka, 'Mobile authentication method', Computer Security Symposium 2004, pp. 625-630 (Oct 2004)

[10] S. Sakurai, T. Munaka, 'Resistance evaluation of user authentication method using matrix against shoulder surfing', IPSJ Transaction, vol. 49, no. 9, pp. 3038-3051 (Sept 2008)

[11] Y. Hirakawa, M. Take, K. Ohzeki, "Pass-Image Authentication Method Tolerant to Random and Video-Recording Attacks", International Journal of Computer Science and Applications, vol. 9, no. 3, pp. 20-36 (2012)

[12] Y. Hirakawa, 'Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks', International Journal of Innovation Management and Technology, vol. 4, no. 5, pp.455-460 (2013)

[13] Y. Hirakawa, T. Itoh, K. Ohzeki, "A New Numerical Password Authentication Method", International Journal of Information Technology and Computer Science (IJITCS), Vol. 12, no. 4, pp.7-15, 2013

[14] J. Kondo, M. Hirano, N. Kamiya, " RM-001: The Strong Authentic Method by Voice Navigation and Relative Value Input eventing from Peeping Attack: Invisible Authentication", FIT Forum, vol. 10(4), pp.33-38, 2011

[15] A. Aratani, A. Kanai," A proposal of authentication methods against shoulder surfing using a sub channel", IEICE Technical Report, vol.114(116), pp.139-144, 2014

Yutaka Hirakawa (M'82) received the Ph.D degree from Kobe University in1991. In 1980, he joined Nippon Telegraph and Telephone Corporation. He is currently a professor of Shibaura Institute of Technology.

His current interests include authentication methods, distributed algorithms,and contents delivery methods.

He is a member of the IEEE computer society, the Institute of electronics and information and communication engineers of Japan (IEICE), the institute of image electronics engineers of Japan (IIEEJ), and Information Processing Society of Japan (IPSJ).

Yutaro Kogure received the B.E. degree in 2015.

His current interests include authentication methods and Internet security.

Kazuo Ohzeki(M'85) received the B.S. degree from Waseda University in 1974, and Dr. of Engineering from Tokyo Institute of Technology in 1999. In 1974, he joined Toshiba Corp. In 1999. He joined Shibaura Institute of Technology, where he has been a Professor.

His research interests include security, video communication, computer vision.

He is a member of IEEE, IEICE Japan, and IPSJ.