fakePointer: A User Authentication Scheme that makes Peeping Attack with a Video Camera hard

Tetsuji TAKADA
National Institute of Advanced Industrial Science and Technology
1-18-13, Sotokanda, Chiyoda-ku, 101-0021, Tokyo, JAPAN
zetaka [atmark] computer [dot] org

INTRODUCTION

In this paper, [1] I propose a novel user authentication scheme that enables to ensure a security against peeping attack with a video camera. Peeping attack is that an attacker steals target's secret by looking into her/his authentication action. In recent days, An attacker uses a video camera to capture a screen and an operation of that action and such incidents have actually occurred[1].

I propose a user authentication scheme, named "fakePointer". It does not leak a user's secret even if an attacker captures target's authentication action by a video camera. The fakePointer has two features to achieve a security against the threat. First feature is a unique user interface for secret input. This makes hard for an attacker to steal a secret from a movie about target's authentication action. Second feature is that an answer operation is randomized in each authentication trial. Users get a randomly generated secret before each trial and use it in inputting their own secret. This makes hard to identify a secret by statistical analysis with multiple authentication movie records. These features realize a more secure authentication scheme against peeping attack with a video camera. This scheme also has no harmful effect to a security level against any other attack methods.

CONCEPT AND USAGE OF THE FAKEPOINTER

In recent days, everyone can purchase a miniaturized video camera with a wireless transmitter and they can conceal it in a place where it seems impossible to install until now. I consider, therefore, that we assume following two situations as practical threats. 1) An attacker has a video record that was recorded both a screen and an operation of victim's authentication action. 2) An attacker may have multiple video records about a same victim.

I think that there are not rare situations. The reason is that ubiquitous and mobile environment forces users to authenticate oneself in a public space and a bad guy may look into your action through a surveillance camera. It means that it becomes hard for us to get a place without a video camera and/or the eyes of other people. We, therefore, need a secure authentication scheme against peeping attack in the real world.

Before starting an explanation of the fakePointer, I put an assumption. It is that peeping attack on a wire, namely wire tapping, is out of the consideration.

I explain a basic concept of the fakePointer using a safety box. A safety box has a dial for inputting a secret number and one marker for pointing to a number. This scheme is clearly vulnerable to peeping attack. Therefore, I put a multiple markers around a dial so as to be always selected all numbers (figure 1 right). And an owner has to determine which markers are used for pointing a secret number. This makes secure against first threat as described before. It is,

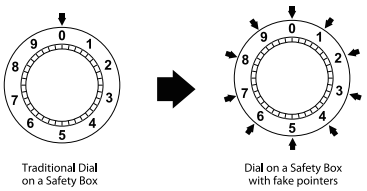

Figure 1. A Dial on a Safety Box with Fake Pointers

however, still vulnerable to the second threat. If an attacker gets multiple authentication video records about a same victim, she/he may correctly identify a victim's secret. The way is that an attacker extracts all possible secret number from each video, and then extracts a frequency of appearance in each possible number. Then, a number with most high appearance frequency would be a victim's secret number.

To ensure a security against this threat, fakePointer introduces a randomized answer input method. A user gets a random disposal secret from an authentication system before start inputting a secret and uses it for answer operation. fakePointer also removes an assumption that a user uses one marker for a secret number input. It means that a user may use four markers to input four digit secret number and the markers are changed in each authentication trial.

I explain an operation procedure in the fakePointer. At first, a user has to get an "answer indicator" before in each authentication. It is an essential information for

[1]This paper was submitted to Annual Computer Security Applications Conference 2007(ACSAC23) for Works in Progress(WiP) session.

inputting a secret and randomly generated by a system. Figure 2 represents an example of an answer indicator. It is composed with four figures in this example. Figure 3 represents a user interface of the fakePointer. The

Figure 2. A sample of an Answer Indicator

Figure 3. A Screen Snapshot of the fakePointer

user interface is composed of two-layered display. Numbers are displayed in the upper layer and ten figures are displayed in the lower layer. The figures in the lower layer are drawn as a background image in each number and they are candidates for an answer indicator.

I explain a secret input operation on the fakePointer. a user already gets an answer indicator and keeps it on a memory. In this explanation, a user's answer indicator is as figure 2. After a user inputs an account name, he/she can see a user interface like figure 3. A user can rotate a layout of numbers on the upper layer by key operation. Left and right arrow keys are assigned in this operation (figure 4).

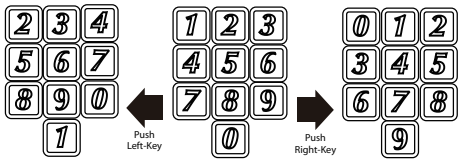

Figure 4. A layout of numbers rotates by key operation

A user moves number layout on the upper layer until his/her first digit of a PIN overlaps first answer indicator figure, and then types a space key. Here is the operation to input one digit of a PIN in the fakePointer. A user, of course, has to repeat these operations until it finishes to input all digits of a PIN. In other words, this operation means that a user has to select **N**th number of a PIN by **N**th figure in an answer indicator. For example, in figure 3, a user inputs a number "9" as a first digit of a PIN because first figure is a "spade" in the figure 2. For this reason, the number of figures in an answer indicator is same with the number of digits in a PIN.

CONSIDERATIONS AND CONCLUSION

I describe about additional advantages and future works of the fakePointer. I think that the fakePointer is a unique authentication scheme because it makes hard for an attacker to steal a secret even if an attacker captures an authentication action as a video record. Moreover, it is also difficult for an attacker to extract a secret even if an attacker got multiple authentication video records about a same victim. The reason is that a randomized answer input with disposal secret makes hard to extract a secret by statistical analysis.

Moreover, the fakePointer has another two advantages in a usability. One is a simple answer input operation. A user can input a secret with just only three keys. It means that the system is easily applicable to a mobile phone. The other is that a memory burden to users is well-controlled to a minimum increase. The reason is that an additional memory burden is a "disposal" answer indicator. I mean that users must remember it only in an authentication because it is a disposal secret and they just remember their secret at normal times.

This project has some future works. One of them is to make an answer indicator to be more easily memorable. I consider that a use of other symbols like numbers, characters or drawings as an answer indicator may become a solution. The other is how to ensure that an attacker can not steal both a video record and an answer indicator of the authentication. The reason is that the situation is an only case that an attacker succeed to get a target's secret in the fakePointer. Some practical solutions should be shown to avoid wrong system implementation.

I finally describe about a status of this work. I have implemented a system prototype and you can try it at a web page. I would like to discuss about security and usability of the system with various areas of people.

REFERENCES

1. Police Department at The University of Texas Austin, ATM Scam - Bank ATMs converted to steal bank customer IDs, http://www.utexas.edu/police/alerts/atm_scam/, Site accessed at Aug 28, 2007
2. Tsutomu MATSUMOTO and Hideki IMAI: Human Identification Through Insecure Channel, Advances in Cryptology - EUROCRYPT 91, Lecture Notes in Computer Science, Springer-Verlag. pp.409-421, (1991)
3. Volker Roth, Kai Richter, Rene Freidinger: A PIN entry method resillient against shoulder surfing, In Proc. 11th ACM Conference on Computer and Communications Security(CCS2004), pp.236-245, October (2004).
4. Desney S. Tan, Pedran Keyani, Mary Czerwinsky: Spy-resistant keyboard: more secure password entry on public touch screen display, OZCHI'05: Proc. of the 19th conference of the computer-human interaction special interest group(CHISIG) of Australia on Computer-human interaction, pp.1-10, (2005).
5. S.Wiedenbeck, J.Waters, L.Sobrado, J.C.Birget: Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme, Proc of Advanced Visual Interface(AVI2006), pp.23-26, May (2006).