fakePointer: 覗き見攻撃に対する耐性を持つ個人認証手法

fakePointer: An Interface for User Authentication that makes Peeping Attack Hard

高田哲司*

Summary. In this paper, 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 victim's secret by looking into a victim's authentication action. In recent days, an attacker uses a video camera to capture a screen and an operation of the action and such incidents have actually occurred.

The fakePointer has two unique features. First is that is provides a unique double layered user interface for secret input. It makes hard to steal a secret even by using a video camera. Second is that an answer operation is randomized in each authentication by using a random secret. These features realize a more secure authentication against peeping attack with a video camera.

1 はじめに

本論文では，個人認証における覗き見攻撃に対する対策として fakePointer と呼ぶ個人認証手法を提案する．既存の個人認証にはいくつかの脅威が存在するが，その一つとして「覗き見攻撃」が挙げられる．この攻撃手法は，攻撃者が正規ユーザの認証行為を覗き見ることでそのユーザの秘密情報 (ex. 暗証番号，パスワード) を奪取する手法であり，種々の脅威の中でも認証システムそのものによる防御が難しいとされる攻撃手法である．また近年，この攻撃手法はビデオカメラを用いて行われるようになり，実際に銀行 ATM で事件が発生するなど，世界的にも社会問題化している．またモバイル，ユビキタス環境の普及に従い，不特定多数の目のある環境下で認証をする機会が今後増大することも予想されることから，この問題に対するなんらかの対策が必要である．

この脆弱性の根本的な原因は，第三者に覗き見られると秘密情報が漏洩するような入力行為をユーザに課しているユーザインタフェースにあると考える．したがって，ユーザインタフェースを改良することで，この問題に対する改善策を見い出すことが可能であると考え，その一つとして fakePointer を提案する．

2 fakePointer の基本概念

現在，誰でも超小型でその映像を無線伝送可能なビデオカメラを購入することができる状況にある．このような状況下において想定すべき脅威は，これまでの人間が覗き見攻撃をするという前提とはまったく異なってくる．本論文では，以下の 2 つの脅威を前提としてその対策手法を考察した．

- 攻撃者は，攻撃対象者の認証画面とその操作を映像記録として保持している
- 同一攻撃対象者の認証行為の記録を複数個保持している

この脅威想定は，実際に発生した銀行 ATM の盗聴事件を基に，盗聴カメラの設置事実が数日間気付かなかった場合を想定して考えたものである．これまでの覗き見対策は，攻撃主体が人間であると仮定されており，それゆえ認証行為全てを人間では掌握できないよう複雑化するという対策手法が提案されてきた [1, 2]．しかしこれらの手法では，正規のユーザの認証行為にも大きな負担を課してしまうという問題がある．しかも，このような手法は上記の脅威想定に対しては意味をなさない．よって我々は，以下の方法で上記の脅威に対して安全性確保を実現する．

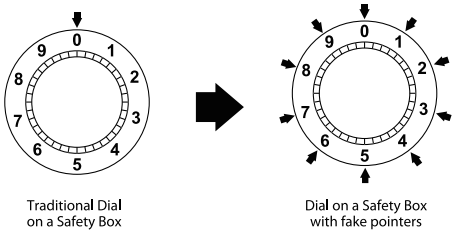

図 1. 金庫のダイアルによる基本概念の説明

その方法を金庫のダイヤルを使って説明する．図 1 左が通常のダイヤル例であるが，これが覗き見攻撃に脆弱なのは，数字を示す矢印が 1 つしかないため明らかである．よって，ダイヤルの全ての数字が常に選択されているように見えるよう，ダイヤルを図 1 右のようにする．これにより覗き見をしている

* Tetsuji TAKADA, 産業技術総合研究所 情報技術研究部門 情報流デザイングループ

攻撃者には入力数値を不明にする．またこの状況において，複数ある矢印のうちの 1 つだけで暗証番号を選択すると仮定すると，複数の認証記録を攻撃者が保有している場合，各記録からすべての暗証番号を抽出し，それらの中から共通する数値を導き出すことによって暗証番号を導き出せてしまう．よって暗証番号の選択には，複数の矢印を使用するものとする．これが fakePointer の基本概念である．

3 fakePointer の実装例

4 桁数字の暗証番号による認証に fakePointer を実装した例について説明する．ユーザは事前に暗証番号を暗記している．この状態で認証する必要が出た際，まずはじめに選択シンボル情報 (図 2) を取得する．

図 2. 選択シンボルの一例

これは金庫の例に例えると「どの矢印で暗証番号を指示するか」を意味する情報となる．この情報は，認証をする度に取得する．それにより，暗証番号の入力方法は認証のたびに変化し，複数の認証に関する映像記録を攻撃者が保持していても，そこから共通する数値を導き出すのが困難になる．

次にユーザ名を入力し，認証画面にアクセスする (図 3).

図 3. 認証画面例

認証画面は二つの表示が重畳した画面になっており，上のレイヤーには数字キーが表示され，下のレイヤーには選択シンボル候補を表す図形群が数字キーの背景画像となるように表示される．このうち上のレイヤーに表示される数字キーは，ユーザの操作によりその配置を一つずつ移動することが可能になっている (図 4).

これを利用し，暗証番号を選択シンボルで指示するのが fakePointer における暗証番号入力方法である．具体的にいうと，自身の暗証番号を選択シンボルに重なるように移動し，その状態で決定キーを押す．図 2 と図 3 を例に説明すると，図 2 の選択シンボルにおいて，画面が図 3 の状態で暗証番号一桁目の決定キーが押された場合，一桁目の選択シンボルは “スペード” なので，“9” が一桁目の暗証番号として入力されたことになる．

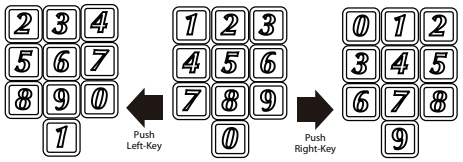

図 4. 数字キーの操作例

4 利点

fakePointer の一番の利点は，これまでの覗き見攻撃に対する対策では想定されていなかった「ビデオカメラで認証行為を撮影される」という脅威に対しても安全性を確保しうる認証手法だという点である．またこの他にも 2 つの利点がある．

1 つは認証操作が単純な点である．認証操作は 3 つのキーのみで行うことが可能であり，第三者に認証行為を覗かれるおそれの高い携帯電話など，入力手段が整っていない環境でも認証操作が可能である．

もう 1 つは，安全性確保のためにユーザに課される新たな記憶負担を必要最小限に抑えている点である．fakePointer では認証の際に選択シンボルを新たに記憶する必要があるが，それは認証操作が完了するまでの間，一時的に記憶するだけでよく，認証が終わったら忘れてもよいからである．つまり認証しない時には，これまでと同様，暗証番号を記憶しているだけでよい．

5 おわりに

本論文では，認証行為をビデオカメラで撮影されても，秘密情報の特定を困難にする認証手法 “fakePointer” について述べた．fakePointer では，二層からなる表示画面を用いた暗証番号の入力インタフェースと，暗証番号の入力をランダム化するため，認証の度に選択シンボルを取得し，それを利用して暗証番号を指示するという二つの特徴により，上記の想定脅威に対する安全性向上を可能した．

参考文献

[1] D. S. Tan, P. Keyani and M. Czerwinsky. Spy-resistant keyboard: more secure password entry on public touch screen displays, *Proceedings of OZCHI 2005*, pp.1-10, 2005.

[2] V. Roth, K. Richter and R. Freidinger. A PIN entry method resilient against shoulder surfing. *Proc. of 11th ACM Conf. on Computer and Communication Security*, pp.236-245, Oct 2004.