fakePointer: 回答候補の複数同時選択による “覗き見攻撃” への安全性改善法 (Revised version)

高田 哲司，増井 俊之

産業技術総合研究所

fakePointer: Improving Security Level against Shoulder Surfing in User Authentication

Tetsuji TAKADA, Toshiyuki MASUI

National Institute of Advanced Industrial Science and Technology(AIST)

1 はじめに

個人認証において，覗き見攻撃[1] に対する対策は急務である．個人認証における秘密情報の入力作業は，第三者に見られない環境で行うことが望ましいが，それは非現実的であると言わざるをえない．また日本では，2005 年末から 2006 年初頭にかけて銀行 ATM における盗撮事件 [1] が発生し，この脅威は広く知れ渡ることとなった．また最近では，画像を用いた認証手法 [4, 5] が提案されているが，これらにおいても覗き見対策は課題の 1 つとなっている．これに対する既存の対策手法は，プライバシーフィルタや遮蔽板の取り付けといった物理的な対策方法 [2] が主流である．しかし，すべての認証端末にこれらの対策を行うのは困難である．

そこで本論文では，画面に表示される選択肢から正解を選択するという操作をする認証を対象とし，覗き見攻撃に対する安全性を改善する手法として fakePointer を提案する．本手法では，ユーザが秘密情報を選択する手法として正解を直接選択するのではなく，fakePointer と呼ぶポインタを使って正解を選択する．fakePointer は，常に複数の回答候補を選択するようになっており，第三者が認証行為を覗き見たとしても，それによりユーザの秘密情報が特定されるという事態を回避可能にする．また fakePointer に ID を割り当てるとともに，それを応用してユーザに回答の一部を偽証をさせることにより，さらなる安全性確保を可能にする．

2 fakePointer

覗き見攻撃を可能にしている一番の原因は，認証時に正解である回答候補を直接選択させているためである．そこで fakePointer では，正解を直接選択させるかわりに，fakePointer と呼ぶ特殊な形状のポインタを用意し，それを使って認証を回答させる．fakePointer は，常に複数の回答候補を選択するため，第三者が認証行為を覗き見たとしても，認証者の秘密情報は特定困難になる．

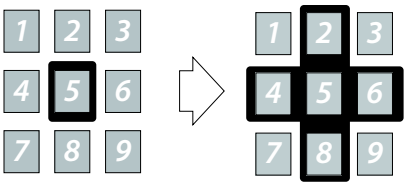

図 1: 従来手法と fakePointer

具体例を示す．図 1 は，銀行 ATM の画面を想定したものである．図中左の図は，既存の ATM で数字の 5 を選択した例である．実際の ATM では図のようなポインタは存在しないが，指で直接選択するかわりに図のようなポインタが存在するとみなすことができる．これに対し fakePointer は，その一例として図中右のような十字型のポインタを使用する．これにより認証画面内の複数の回答候補が選択された状態になる．図の例では **2,4,5,6,8** の 5 つの回答候補が選択されており，これを第三者が覗き見たとしても，ユーザの選択した回答がそのうちのどれなのかが不明となる．

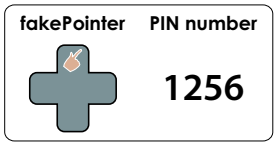

図 2: 正規ユーザの秘密情報

一方，正規ユーザは，十字ポインタ内の特定部分[2] で自分の秘密情報を選択し，回答を行う．つまり正規ユーザは，図 2 のように fakePointer の形状と，正解選択用の位置に関する情報を事前に知っているものとする．

なお fakePointer の移動により，ポインタの一部が認証画面を逸脱することが考えられるが，その場合には逸脱した部分を折り返すことで対処する．図 3 に例を示す．図中の上と中の例は，ポインタの一部が画面右および上に “はみだした” 例であ

[1] shoulder surfing, observation attack とも言われる

[2] 自明だが，十字ポインタの場合は 5 つの選択可能部分がある

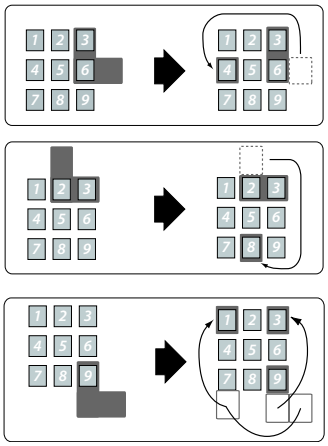

図 3: 認証画面を逸脱したポインタの折り返し処理例

る．これらの場合，はみだした部分は折り返されて認証画面の左および下の部分を選択することになる．図中下の例は，はみだした部分の 1 つが右下にはみだしているが，これも同様に 2 回折り返し処理をすることにより左上の “**1**” を選択することになる．これにより fakePointer のどの部分であっても全ての回答候補が選択可能になる．したがって，図 2 の秘密情報を持つユーザが認証に回答する場合は，図 4 のようになる．

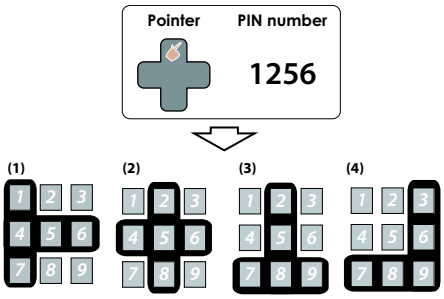

図 4: fakePointer による認証回答例

2.1 ID 割り当てと偽証の導入

本手法はこのままでは問題がある．理由は，fakePointer を使用しても，覗き見により攻撃者が得られる秘密情報の数は少なく，安全性を確保できないからである．図 5 を用いて説明する．

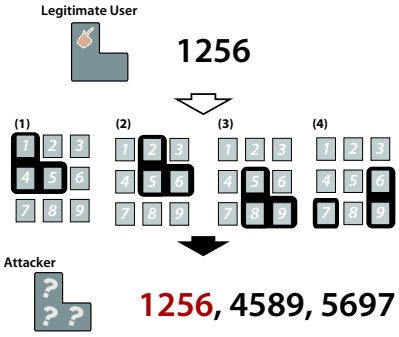

図 5: 覗き見により攻撃者が得る情報

ここでは L 字形の fakePointer を例にとる．図 5 は，正規ユーザが **1256** という暗証番号を入力した例である．しかし，攻撃者がこれを覗き見ていた場合，fakePointer のそれぞれの選択位置に対応する回答を読みとることで，**1256, 4589, 5697** の 3 つの秘密情報候補を得ることができてしまう．回答候補が 3 つでは，既存の銀行 ATM でも “なりすまし” に必ず成功する[3]．よって，覗き見攻撃に対する安全性はないことになる．また fakePointer が画面内のすべての回答選択肢を選択する形状だとしても，図 5 の認証画面では最大で 9 個しか攻撃者に暗証番号候補を与えることができず，1/3 の確率で “なりすまし” に成功することとなる．これでは，覗き見攻撃に対する安全性を向上させたとは言えない．

そこで我々は，fakePointer に ID を割り当て，かつ，その ID 値を利用してユーザに “偽証” させる仕組みを導入する．詳細について説明する．ここでは，fakePointer の選択可能場所数を **Pn** とする[4]．この条件で，ポインタの各選択位置に **1** から **Pn+1** までの数字を ID として用意し，その中から **Pn** 個の ID を重複することなく割り当てる．図 6 はその一例である．

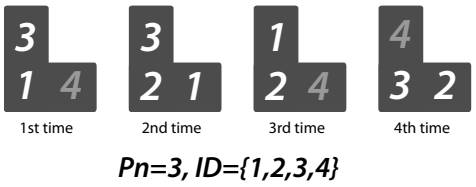

図 6: ID 付き fakePointer: L 字形ポインタの場合

正規ユーザは，どの ID の位置で秘密情報を選択すべきかを事前に知っているものとする．回答方法は，その正解選択用の ID 値が fakePointer 内に存在するかによって，以下の 2 通りとなる．

1. ID が存在する場合，該当 ID の位置で秘密情報を選択する．
2. ID が存在しない場合には，どの回答候補を選択してもよい．

図 6 の例で説明する．ここでは，正解回答用 ID を **4** とする．2nd time を除く 3 回の回答は，fakePointer 内に ID=**4** が存在するので，その位置で秘密情報を選択する．ただし，2nd time の場合は，正解選択位置を示す ID が存在しないので，ユーザは何を選択してもよく，それは正解となる．これによりユーザは，4 回の回答のうち 1 回だけ嘘 “かもしれない” 回答をすることになる．これにより，認証行為を覗いていた攻撃者に与えることのできる秘密情報の候補数は増加する．覗き見ていた攻撃者が得る秘密情報の数は以下のようになる．

偽証を含む回答の数 x **偽証のかわりに正解となりうる回答候補数**

図 7: 攻撃者に与えうる秘密情報の数

図 6 の例では $4 \times 9 = 36$ 通りとなる．

これにより，覗き見攻撃に対する一定の安全性を確保しうるものと考える．しかし，これでもまだ欠陥がある．理由は，本手法の導入により，Brute-force 攻撃に対する安全性が低下するためである．具体的に言うと，ユーザがとりうる秘密情報を，攻

[3] 既存の銀行 ATM は 3 回認証を試行することができるため
[4] L 字形ポインタなら 3，十字形ポインタなら 5 である

撃者が “しらみつぶし” に調べる場合，調査すべき秘密情報の数は，暗証番号のうち 1 桁分が意味をなさなくなるため，9^4 個から 4×9^3 個に減少するからである．

覗き見攻撃に対する対策のために，Brute-force 攻撃に対する安全性が下がることは許されない．よって，その低下分を補う必要があるが，その方法として一番簡単な方法は，回答回数を 1 回増やすことであり，暗証番号ならば，暗証番号の桁数を 1 つ増やすこととなる．これが本提案手法において，安全性を向上させるためにユーザが負担しなければならないコストであると言える．

3 考察

本章では，本手法にて明確にしていない点について言及するとともに，応用例として One-Time Password 化を提案する．さらに関連研究について述べる．

本提案手法には，2 点ほど明確にしていない要素がある．1 つめは fakePointer の形状である．fakePointer の形状は，複数の回答候補を選択しうる形状であれば基本的に自由である．ただし，ID 割り当ての都合上，fakePointer は，(1 回の認証における回答回数 − 1) 以上の選択位置を持つ必要がある．

2 つめは，fakePointer 情報の取得/通知方法である．これに関して我々は，通知方法に厳格な機密性がなくても運用は可能であると考える．その理由は，仮に fakePointer に関する情報が第三者に知られることになったとしても，認証の秘密情報自体が第三者に知られない限り，それが即座に “なりすまし” につながらないからである．なぜならば，fakePointer は秘密情報の一部であり，それだけでは，認証を成功させるための十分条件ではないからである．銀行 ATM を例に考えると，暗証番号が攻撃者に知られない限り，fakePointer に関する情報が攻撃者に知られたとしても認証の安全性は保たれるということである．本手法は，あくまで覗き見攻撃に対する安全性改善手法であり，認証における安全性は，本手法を導入する認証手法によって確保される．よって，fakePointer の取得/通知に関しては，より簡単な認証や電子メールによる通知でも問題にはならないと考える．

3.1 疑似 One-Time Password 化

fakePointer 取得/通知の機密性に関する前述の特徴を利用することで，提示選択型認証を擬似的に One-Time Password 化することが可能となる[5]．その手法について説明する．

認証システムは fakePointer の形状を複数種用意しており，ユーザからの fakePointer 発行依頼を受けて，その中からランダムに形状を選択し，ID 値を割り当てて発行する．発行された fakePointer は，1 回の認証でのみ使用可能とする．つまり，認証を行うユーザは，認証のたびに fakePointer の発行を受ける必要がある．また fakePointer は，各ユーザに対して常に 1 つだけ発行されるものとし，以前発行された fakePointer は，それが未使用であっても新たな fakePointer が発行された時点で無効となる．これらの規則を導入することにより，fakePointer が秘密情報のランダム化を果たすことになり，結果として，既存の認証を擬似的に One-Time Password 化することが可能になる．

またこれにより，2 つの利点が得られることとなる．1 つは，記憶負担の軽減である．この枠組により，ユーザは fakePointer に関する情報を記憶する必要がなくなる．結果として，ユーザに新たな記憶負担を課すことなく，認証における安全性を向上させることが可能となる．もう 1 つは，安全性の強化である．本手法の導入により，Brute-force 攻撃に対する安全性の低下について指摘したが，One-Time Password 化によりその安全性の低下を補うことが可能になる．なぜならば，認証時に fakePointer の形状を選択する必要が生まれることから，回答回数が 1 つ増加するためである．(図 8).

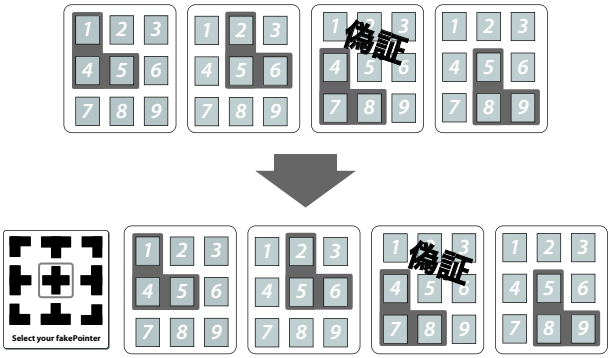

図 8: Pointer 選択画面の追加による認証手順の変化

つまり，fakePointer の形状数が，それ以降の認証画面の回答候補数以上であれば，この fakePointer 選択が，偽証による回答無効分の代替となり，結果として brute-force 攻撃に対する安全性は維持されることとなる．またこの対策は，覗き見不可能な攻撃者に対して，brute-force 攻撃に対する安全性が向上させることにもなる．なぜならば，覗き見をしてない攻撃者にとっては，暗証番号も不明な上に fakePointer の形状も不明なためである．

3.2 関連研究

画像認証の分野でいくつか提案されている “覗き見攻撃” に対する対策手法を紹介する [6, 8].

論文 [6] では，画像認証で使われる画像に画像処理を施すことで，一見しただけではなんの画像かわからないようにして認証に使用する方法を提案している (図 9)．正規ユーザは，原画像からその不鮮明化画像に至るまでの画像処理の過程を見ることで，その不鮮明化画像を記憶することができ，結果として認証時にはそれを正確に判別可能することが可能になる．

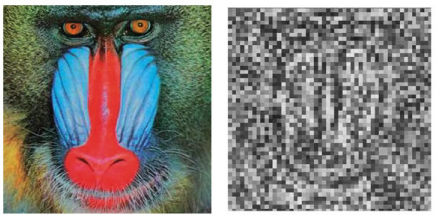

図 9: Original and Processed Images

[5] “擬似的” という意味は，一度発行された fakePointer が二度と使用されないことを保証しないため，厳密な意味で One-Time Password ではないという意味である

またユーザ評価により，複数枚の画像群の中からパスワード画像の判別が可能であることを実証している．しかし，被験者が限定されているため，結果は普遍的とは言い難く，また長期記憶や利便性の面からも疑問点が残されているといわざるを得ない．

論文 [8] では，事前に pass-object と呼ばれる特定のアイコンを複数個決めておき，認証時には画面に 3 つの pass-object が表示されるので，その pass-object で構成される三角形の内部にあるアイコンを回答として選択する (図 10)．これを複数回行い，すべての回答があっていれば認証成功とする手法である．

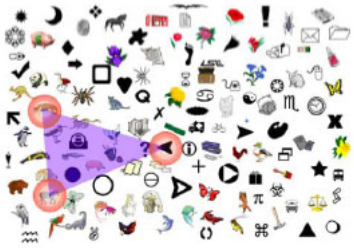

図 10: A shoulder-surfing resistant graphical password scheme

この手法は Challenge & Reponse になっており，かつ正解を直接選択しないという点で優れているが，多数 (数百〜数千) の object が画面に表示されることが前提となるため，pass-object の識別が容易とは言い難く，また認証時間も長くなることが予測される．また pass-object の数やその配置にも依存するが，画面の中心を回答として選び続けることで認証に成功する可能性が高くなるという可能性もある [9]．

これに対し本手法では，覗き見攻撃に対する対策手法として，「見られないようにする」のではなく,「見られても一定の安全性を確保可能にする」手法として新たな手法である．また本手法は，提示選択型の認証であれば広く適用可能な安全性改善法であり，それは既存の銀行 ATM の認証でも適用可能であるということはこれまでの説明からも明らかである．また本手法の導入に際し，One-Time Password 生成のために乱数表や特定のハードウェアをも持つ必要もない．

また本手法では，安全性を向上させつつも，ユーザに課される負担を増やさないように配慮している．銀行 ATM を例にとると，安全性向上のためにユーザに課される記憶負担の増加は，fakePointer に関する情報は記憶しなくても運用可能なため，数字 1 桁分だけである．またその操作性は，既存の提案手法と比較しても大きく変わるものではないと言えるだろう．また本手法の応用により，既存の認証手法をその枠組を大きく変化させることなく One-Time Password 化することも可能であり，それにより Brute-force 攻撃に対する安全性強化も可能となる．

4 おわりに

本論文では，提示選択型個人認証における “覗き見攻撃” への安全性を改善する手法として fakePointer を提案した．fakePointer とは，認証時に回答を選択するポインタだが，それは常に複数の回答候補を選択する形状となっている．正規ユーザは，認証時に使用する fakePointer の形状と，正解を選択する位置を示す ID 値を事前に知っており，認証時には，種々の形状から正しい fakePointer を選択し，かつポインタに割り当てられた ID のうち正解選択位置を示す ID の位置で，自身の秘密情報を入力することで認証を行う．ポインタに割り当てられる ID は，ポインタの選択可能場所数を **Pn** とすると，**1〜Pn+1** の中から Pn 個がランダムに割り当てられる．ユーザは，自身の正解選択位置用の ID が fakePointer 内に存在する場合には，その位置で正解を選択し，fakePointer 内に ID が存在しない場合には，なにを回答してもよいものとする．これにより攻撃者が認証行為を覗き見ていたとしても，それにより得られる回答候補が一定の数となり，ユーザの秘密情報の特定を困難にする．

本手法は，既存の銀行 ATM でも適用可能な方法であり，かつ既存の認証を One-Time Password 化することも可能にする．また本手法の適用による操作性や記憶に対する負担は，提案されている既存の対策手法と比較しても少ないといった特徴を持つ手法である．

参考文献

[1] ATM 盗撮事件, Yahoo! Japan News, http://dailynews.yahoo.co.jp/fc/domestic/atm_sneak_shot/, site accessed at Apr 10, 2006.

[2] トマト銀行，操作画面すっぽり覆う「盗撮防止カバー」を ATM に設置, ITPro, http://www.nikkeibp.co.jp/wcs/leaf/CID/onair/jp/it/425911, site accessed at Apr 10, 2006.

[3] オンラインバンキング利用者を対象としたセキュリティ意識調査結果を発表, RSA Security, http://www.rsasecurity.com/japan/news/data/200603241.html, site accessed at Apr 12, 2006.

[4] Rachna Dhamija and Adrian Perrig: Deja Vu: A User Study Using Images for Authentication, 9th Usenix Security Symposium, Aug (2003). http://www.sims.berkeley.edu/%7erachna/dejavu/ site accessed at Apr 17, 2006.

[5] 高田哲司，小池英樹: あわせ絵: 画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法, 情報処理学会論文誌，Vol.44, No.8, pp.2002–2012, (2003).

[6] 原田篤史，漁田武雄，水野忠則，西垣正勝: 画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46, No.8, pp.1997–2013, (2005).

[7] 荒川豊，竹森敬祐，笹瀬巌: 入力位置情報を付加したパスワード認証方式，コンピュータセキュリティ研究報告，情報処理学会，Vol.2003, No.45, pp.35–40, (2003).

[8] L.Sobrado and J.-C.Birget: Graphical passwords, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol.4, (2002). http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm site accessed at Apr 17, 2006.

[9] S.Man, D.hong and M.Mathews: A shoulder-surfing resistant graphical password scheme - WIW, in proceedings of International Conference on Security and Management, Las Vegas, NV, (2003).