画像認証に対して未利用者が受ける印象に関する調査

高田　哲司[1]

産業技術総合研究所 情報技術研究部門[1]
〒135-0064 東京都江東区青海 2-41-6

知識照合型個人認証の問題点を改善しうる認証手法として，画像を利用した認証が提案されている．しかしそれらの認証手法は，なんらかの理由により普及に至っていないのが現状である．そこで本論文では，画像認証においてその普及を阻害している要因を調査する目的で，そのような認証を利用したことのないユーザに対してアンケート調査を実施した．その結果，認証システムが使用する画像種に関してはユーザが敬遠する傾向の高い画像種が明確になった．またその他にも，いくつかの設計要素に関して興味深い示唆が得られた．これらの調査結果は，今後の画像認証システムにおける設計や既存の画像認証の改善において設計方針を決定する際の指針として利用されることが期待される．

An Investigation of First Impressions to Image-based Authentication Systems in Unexperienced Users

Tetsuji TAKADA[1]

National Institute of Advanced Industrial Science and Technology[1]
2-41-6 Aomi, Koto-Ku, Tokyo, 135-0064, JAPAN
E-mail: zetaka @ computer . org

In this paper, I describe about a user perception of image-based authentication systems. The purpose of this work is to extract positive and negative factors in their systems. And I consider that they will help to design a better image-based authentication systems and give a better direction to improve a system. To do that, I conducted a survey on graduate students that are inexperienced in such authentication systems. I asked them to make a ranking of five systems after I had given a lecture about them. I show a result and discuss about some indications to realize a better image-based authentication systems.

1. はじめに

近年，パスワードや暗証番号のかわりに画像を秘密情報として利用した認証システムが提案されている[1)~5)]．これらの認証システムは，知識照合型認証方式の問題点を改善しうる新たな認証手法として，その普及が期待されている．しかし，現時点での状況を見る限り，その普及が進みつつあるとは言えない状況にある．

その要因は複数あると考えられる．概念や理論のみで利用可能な実装がない．システム提供側またはユーザ側に認証システムを変更するほどの動機やニーズがないなど様々な要因が考えられる．そういった要因の1つとして，ユーザが新たな認証手法に対して否定的な印象を持ち，敬遠してしまうという点もあると考える．利用可能な実装が存在し，選択肢の1つとしてその利用が開始されたとしても，利用者がそれに対して否定的な印象を抱いてしまった場合，それを覆して普及に至るのは困難であると予想され，認証システムの普及に対する阻害要因となる可能性がある．

そこで本論文では，既存の画像認証には阻害要因が存在すると仮定し，その要因を明確にすることを目的として調査実験を行った．この調査のため，被験者としては画像を利用した認証システムを利用した経験のない大学院生を対象とし，既に提案されている画像認証システムに対し，彼らがどのような印象を持つかをアンケート調査することにより，その把握を試みた．この結果をまとめ，その内容について議論することにより，その普及を妨げていると推測される画像認証システムの設計上の要因の抽出を行った．

以降本論文では，2章で本調査における調査方法について説明し，3章で調査結果を整理する．最後に4章で実験結果に対する考察を行い，得られた調査結果から明確になった阻害要因について議論する．

2. 調 査 方 法

本章では，本研究で実施した調査方法について説明する．画像認証に対してエンドユーザが抱く印象を調査するため，2007 年 10 月に大学院の講義において画像認証に関する授業を 90 分実施し，その後にレポート課題としてアンケートの提出を求めた．アンケートに応じた被験者は 40 名で，性別と年齢構成は 20 歳代男性 34 名/女性 5 名および 30 歳代 男性 1 名であった．なお被験者は全員が情報系の大学院生であり，既存の認証システムを日常的に利用しているが，画像を利用した認証を使用した経験を持つ者はいなかった．

アンケートにおいて被験者に課した課題は次の通りである．被験者に対して画像を利用した認証システムを 5 種類提示し，あわせてその詳細を知ることができるような資料へのリンクを提示した．ここでいう資料とは，学術論文またはその認証システムの仕組みを解説している Web ページである．これらを熟読して仕組みを理解した上で，これらの画像認証システムを自分が利用したいと思う順に順位付けし，またその理由について簡単に述べよ．という課題を課した．またこの順位付けに関する理由の他に，画像認証に関して意見があればその旨を記載せよという項目も用意した．被験者からの回答例を図 1 に示す．

情報セキュリティ講義 画像認証レポート

学籍番号:07SXXXX
性別: 女性
年代: 20歳代

○ 1位 画像なぞなぞ認証
☆ 理由
何かと何かを自分ルールで関連付けるのは好きなので。
リマインダの画像版という印象があります。

○ 2位 モザイク認証
☆ 理由
他人にばれにくそうなので、信頼性が高ければ使いたいです。

○ 3位 あわせ絵
☆ 理由
画像を用意するのが面倒かもしれないが、覚え易そうなので。
桁を増やしても記憶が難しくならないのが嬉しいです。
操作は面倒になりそうですが。

○ 4位 ニーモニックガード
☆ 理由
イラストが親しみ易そうなので。
しかし、ストーリー仕立てにするのは覚えにくそうです。
写真を並べるのはひねりのない印象。

○ 5位 Deja Vu
☆ 理由
抽象的な模様が覚えられそうにないので。

■ 意見，質問，感想等
世の中には色々とユニークな認証方式があるようなので、
有効度の高いものは、世の中に広まって欲しいです。

図 1 アンケート回答例

2.1 対象とした画像認証システム

本節では本調査実験で評価対象とした画像認証システムについてそれぞれ簡単に説明する．

2.1.1 Deja Vu

画像認証システム Deja Vu[5] は，Rachna らが提案しているシステムであり再認型の画像認証システムとして著名なシステムである．ユーザは事前に 5 つのパスワード画像を決定しておき，認証時には認証画面に提示される 20 枚の画像の中から順不同で自分のパスワード画像を正しく選択することで検証を行う認証手法である．また本手法では，システムで使用する画像を「ランダムアート画像」としており，それにより推測攻撃に対する安全性を確保している．図 2 は Deja Vu による認証画面の一例である．

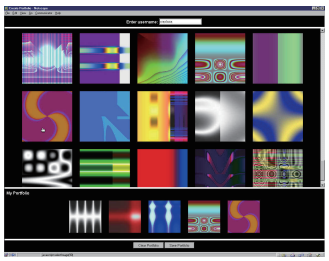

図 2 Deja Vu の認証画面例

2.1.2 IQ-Auth:画像なぞなぞ認証

IQ-Auth[3] は，増井によって提案されている画像認証であり，他の 4 つの認証システムとは異なり，画像そのものをパスワードの代替として使用するのではなく，パスワードのリマインダーとして画像を利用している認証システムである．

認証方法について説明する．ユーザは好きな画像を選択し，その画像を見れば回答が想起できるような “なぞなぞ” を考案する．その “なぞなぞ” の答えと，おとりの回答選択肢として複数の回答候補を用意し，画像とともに登録する．これがパスワードの設定に該当する．認証時には図 3 にあるような認証画面が出現する．ここで表示される画像から想起される正しい回答を複数の回答選択肢の中から選択する．この行為を認証に求められる安全レベルにあわせた回数分繰り返し，すべての回答が正解ならば正規のユーザとみなす．という認証手法である．

図 3 Deja Vu の認証画面例

2.1.3 ニーモニックガード

ニーモニックガード[4] とは (株) ニーモニックセキュリティが発売している認証手法であり，Deja Vu と同様の仕組みにより認証を行う認証方法である．本手法の特徴は，Deja Vu とは異なり使用する画像に制約が

ないことと，回答は順不同ではなく回答順序も検証されるという点である．したがって，複数のパスワード画像をその回答順序も含めて記憶する必要がある．その記憶を支援するため，決定したパスワード画像の入力順にあわせて適切なストーリを作成し，それを用いてパスワード画像とその入力順序の記憶補完をすることを推奨しているという特徴を持つ．

2.1.4 あわせ絵

あわせ絵[1]は高田らが提案している手法で，2つの特徴がある．1つはユーザ自身が撮影した写真を認証に使用することであり，もう一つは認証画面内に正解がないという事象を組み込んだことである．またDeja Vu[5]やニーモニックガード[4]とは異なり，1つの認証画面で全ての回答を行うのではなく，回答のたびに認証画面が新たに生成される仕組みとなっている．図4は，あわせ絵の認証画面例である．

図 4 あわせ絵の認証画面例

2.1.5 画像記憶のスキーマを利用したユーザ認証システム

「画像記憶のスキーマを利用したユーザ認証システム」[2]は原田らが提案している手法で，認証時に使用する画像に対して画像処理を施すことにより，覗き見攻撃の脅威に対する安全性を確保した画像認証システムである．ユーザはパスワード画像を決定した後，それを認証で使用する加工済み画像に至るまでの画像処理過程を事前に学習し，記憶する．認証時には図5のような認証画面が提示されるので，その中から自身のパスワード画像を選択する．それを必要な回数繰り返し，すべての回答が正解であれば正規のユーザとみなす認証手法である．

なおこれらの認証システムを評価対象として選択した理由は，再認手法による画像認証システム，つまり画像そのものを秘密情報とし，それを認証時に認識/選択することで回答を行う認証システムに強い興味を持っており，その方式による認証手法に適用されている様々な設計要素に関して評価を行いたいという意図があったためである．したがってvisKey[6]などに代表されるCued-based authentication[7]つまり「画像内の特定の位置を秘密情報とする」認証手法やCAPTCHA[8]は今回の実験では評価対象として採用しなかった．

図 5 画像記憶のスキーマによる認証画面例

3. 調査結果

調査結果について述べる．なお以降では「画像記憶のスキーマを利用したユーザ認証システム」を“モザイク認証 (Mosaic Auth.)”と呼ぶこととする．

図6に回収したアンケートを集計した結果である．この図は，各認証手法に対して各順位を付与した被験者数の分布を棒グラフとして表したものである．また図7は，各認証手法毎に1位から各順位までのランキングを付与した被験者の累積数を折れ線グラフとして表したものである．図7中の各折れ線グラフには5つの値を示すプロット点があるが，一番左の値は各認証手法を1位とランク付けした被験者の数を示し，左から二つ目の値は1位と2位にランク付けした被験者の合計数を示している．したがって一番右の値は，各認証手法において1位から5位までランク付けした被験者の合計数，すなわち全被験者数となる．

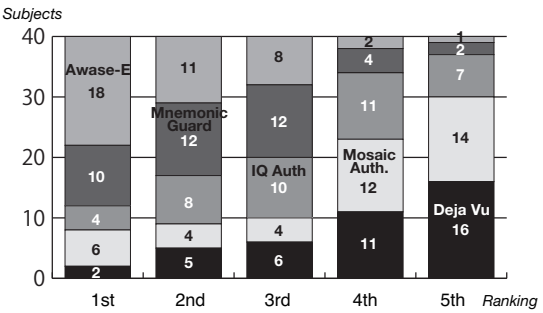

図 6 各認証手法の順位別 被験者数分布図

図6の結果から，これら5つの認証手法は以下の3つのグループに分類できる．この分類は，図7において1位から何位までの被験者数の総和が被験者の50%を超えるかという点について着目すると明確

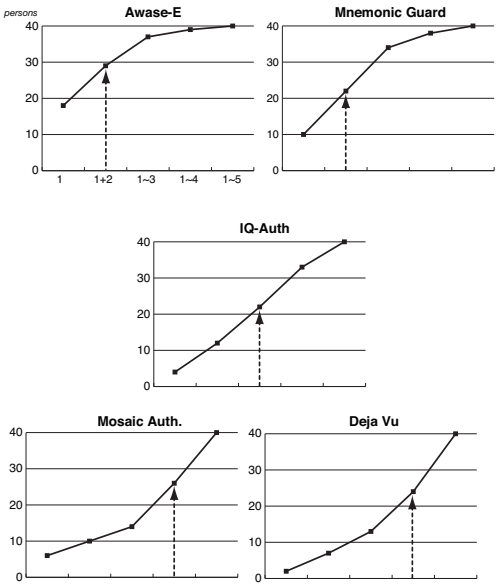

図 7 各認証手法別 累積被験者数のグラフ

になる．

- おおむね肯定的:
  あわせ絵，ニーモニックガード
  (1 位と 2 位の和で被験者数の 50%を超過)
- どちらかというと否定的: モザイク認証，Deja Vu
  (1 位から 4 位までの総和で被験者数の 50%を超過)
- どちらともいえない手法:
  IQ-Auth
  (1 位から 3 位までの和で被験者数の 50%を超過)

以降では，各認証手法のうちのいくつかを抽出し，それらについて比較調査した結果について述べる．

あわせ絵とニーモニックガード

これらは肯定的に評価された認証システム群である．それぞれを 1 位と評価した被験者数を見ると あわせ絵：ニーモニックガード = 18：10 となり，あわせ絵の方がニーモニックガードよりも肯定的に捉えられている．しかし，全体的にこの両者がどのように評価されているかを知るため，全てのアンケートからあわせ絵とニーモニックガードの評価値のみを抽出し，どちらが肯定的に受け止められる傾向にあるのか，その値を直接比較した．つまりある被験者の評価が，あわせ絵が 4 位でニーモニックガードが 3 位だった場合，ニーモニックガードの方があわせ絵よりも肯定的に認知されているという結果になる．以降本論文では，この方法による比較方法を「直接比較」と呼ぶことにする．この方法でアンケートを集計した結果，あわせ絵の方を好む被験者が 26 人であるのに対し，ニーモニックガードの方を好む人は 14 人という結果になった．したがって，全体的に見てもあわせ絵の方がニーモニックガードよりも肯定的に受け止められていると見ることができる．

モザイク認証と Deja Vu

これらの手法はどちらかというと否定的に評価された認証システム群である．Deja Vu とモザイク認証について 5 位の被験者数を比較すると，モザイク認証:Deja Vu= 14：16 と大差はない．また前述同様，双方の認証手法において直接比較を行った結果は，モザイク認証の方を好む被験者数が 21 人に対し，Deja Vu の方を好む人が 19 人という結果になった．これらの結果から，どちらがより否定的に受け止められているかを判定するのは困難という結果になった．

IQ-Auth とあわせ絵，ニーモニックガード

あわせ絵とニーモニックガードは IQ-Auth より好まれる傾向にあることは評価結果からも見てとれる．1 位と評価している被験者数でもそれは明らかであるが，直接評価の結果もそれを支持する結果となった．あわせ絵と IQ-Auth との直接比較による結果は，あわせ絵:IQ-Auth= 30 : 10 であり，ニーモニックガードと IQ-Auth との直接比較による結果もニーモニックガード:IQ-Auth= 30 : 10 と，双方ともに 3 倍もの差が現れる結果となった．

IQ-Auth とモザイク認証，Deja Vu

IQ-Auth がモザイク認証や Deja Vu よりも好まれる傾向にあることは，評価結果からも明確である．しかし，これらの手法を直接比較したところ，興味深い結果が得られた．IQ-Auth と Deja Vu による直接比較は，$IQ - Auth : DejaVu = 27 : 13$ となり，2 倍以上の差があることからその傾向は明らかだが，IQ-Auth とモザイク認証に関する直接比較の結果は，$IQ - Auth$: モザイク認証 = 24 : 16 となった．値としては IQ-Auth の方が好まれる結果ではあるが，その差は再検討に値すると解釈しうる結果であると考える．

女性特有の傾向

女性の被験者数は前述の通り 5 人のため，本調査結果をもって女性一般に見られる傾向と論じることはできない．しかし本調査から得られた女性に特有と推測される傾向について述べておく．表 1 は，女性被験者のみによる実験結果の集計である．

注目したいのは女性がニーモニックガードに一定の支持を示している点であり，2 位までの集計まで考慮すると IQ-Auth も一定数の支持を集める可能性があるという点である．これは女性が “ストーリ” や “なぞなぞ” の作成に対する拒否反応が少ない傾向にあることを示していると解釈できる可能性がある．またこの事実を裏付けるように，3 名の女性被験者が，アンケートにてその旨を明記していた．絶対数が少ないためあくまで可能性ではあるが，半数以上の被験者がそういった行為に肯定的な意見を示しているのは興味深

表 1 女性被験者による評価結果

	ニーモニックガード	あわせ絵	IQ-Auth	モザイク認証
1 位の被験者数	3	1	1	0
1 位と 2 位の被験者数の和	3	4	2	1

い結果である．

また各認証手法に対して寄せられたコメントについて，その概略を述べる．

- あわせ絵: 肯定的な意見としては，自分の撮影した写真が使えることに関する指摘が多く，否定的な意見としては，推測攻撃ならびに覗き見攻撃に対して脆弱に見えるという指摘が多数であった．
- ニーモニックガード: 肯定的意見としては，イラストや写真といった画像を利用しているため，記憶可能性に関しては肯定的な意見であった．しかしその一方で，ストーリ付けによる記憶補完は困難であるという意見が少なくなく，12 名もの被験者がその点を明記していた．
- IQ-Auth: 否定的な意見としては，“なぞなぞ” を考えるのが面倒だという意見が多数であった．しかしその裏返しとして，それができれば安全性は高いであろうという指摘が肯定的意見として寄せられており，その評価を示す数値として，直接評価の結果，あわせ絵よりも IQ-Auth の方を肯定的に評価する被験者は 10 名もいた．
- Mosaic Auth.: 肯定的な意見としては，覗き見攻撃に対する安全性は高いであろうという指摘が 8 名ほどあった．一方否定的な意見としては，false negative に対する懸念，つまり正規ユーザが認証に失敗する確率が高くなりそうだという意見が 17 名もの被験者から寄せられていた．また 11 名もの被験者が画像種そのものに対する嫌悪感を明記していた．
- Deja Vu: パスワード画像の記憶は困難であるという否定的な意見が大多数であった．しかし利用開始時の負担が少ないという肯定的な指摘もあった．

4. 考　　察

実験結果に対する考察を述べる．まずはじめに本調査を通じて明らかになった設計要素は，画像認証で使用する画像種に関する点である．画像認証で使用する画像は写真やイラストなどその内容が自然であり，かつ人工的な加工を加えていない画像の使用が望まれる傾向にあり，人工的に生成された画像や事後に人工的な加工を施した画像を使用する認証手法は，たとえそれが安全性向上に効果があるとしても否定的に受け止められる傾向にあることが明らかになった．

これは認証に画像を利用する第一の目的が，その記憶支援にあることを考慮すると妥当な結果であるといえる．この点については画像認証を使用したことのないユーザであっても的確に評価を行っていることが明らかになった．

またアンケート結果から，以下のような興味深い示唆も得られた．

1 つめは，Mosaic Auth. と Deja Vu へのコメントにおける想定脅威への反応の差である．Mosaic Auth へのコメントには「覗き見攻撃に対する安全性」に関するコメントが見受けられたのに対し，Deja Vu における推測攻撃への安全性に対するコメントは 1 つもなかった．これは画像種を人工的なものにしても安全性を向上させるという設計要素に対して，覗き見攻撃に対しては被験者は反応を示したが，推測攻撃に対しては反応を示さなかったということになる．この事実は，1) 推測攻撃よりも覗き見攻撃の方を現実的な脅威と認識している．2) ランダムアート画像の記憶可能性に関する懸念が大きく，それにより得られる利点に評価が至らなかった． 3) 人工的な画像の利用は覗き見攻撃対策なら許容されるが，推測攻撃対策としては許容されない．のいずれかであると考えられ，これについてはさらなる調査が必要である．

2 つめは IQ-Auth と Mosaic Auth の比較である．全体的には IQ-Auth の方が肯定的に評価されているものの，直接比較ではその差は小さく，再調査に値するほどであった．これは「画像記憶のスキーマによる記憶」と「画像から連想される知識記憶」のどちらが実行可能性が高いと感じられたかという比較になると考える．これも追加調査が必要な項目であると考える．

3 つめはストーリ作成による記憶補完に対する印象である．この設計要素に対する一般的な評価は否定的であることは事実である．しかし注目すべきは，女性被験者の半数が “ストーリ” や “なぞなぞ” 作成に対し否定的ではない旨を明記したという事実である．この事実は，被験者の絶対数が少ないため一般化はできない．これはより多くの被験者により再調査を行い，これが一般的な傾向と言えるかを確認する必要があると考えている．またストーリ作成による記憶補完は，その運用が困難であるという実験結果がすでに存在するが [9]，このような意向を表明をしている被験者に対し，実際にストーリ作成による記憶補完を用いる認証システムを使用させ，使用の前後でその印象がどう変化するかという実験を行うことも検討に値すると考える．

最後にこのような実験の意義について述べる．実際にシステムを用いた評価実験ではなく，単に知識を与えた上で，その「印象」を調査することがセキュリティシステムの向上に対して意義のあることかという点については議論の余地がある．しかしセキュリティシス

テムもそれを人間が使用する以上，なんらかの機能的向上が実現されたとしても，それが人間にとって使用に耐えないシステムでは意味がない．もちろんシステムに必要な安全性を犠牲にしてでもユーザに受け入れられるシステムを歓迎するわけではない．大切だと考えるのは，システムの開発や改善のプロセスにおいて必要要件を満たすためにユーザの受容性を大幅に減じてしまうような選択肢を採用してしまわないような指針を提供することである．もしそのような指針があれば，システムの設計時に複数ある選択肢から必要な機能は実現できるがユーザのシステム受容性を大きく減じるような選択肢を回避したり，最小限の受容性低下にて必要な機能の実現を可能にする選択肢を選択することが可能になると期待できるからである．もちろん論文 [10] のように， ユーザがシステムに対して抱く印象と実際にシステムを使用した後の評価が異なることもあり，本調査結果が普遍的な指針になりうるとは言えないことも事実である．本研究はこれまでの様々な研究成果を否定するものではなく，画像認証の普及に向けて，どのような設計要素はその採用を避けた方がよいかをユーザ視点で示すことである．Incentive-Centered Design(ICD) という設計手法がある [11]．これは人間をシステムにおける自律コンポーネントとしてとらえ，それらがシステムにとって望ましい行動をとるようにシステムを設計するという手法である．画像認証では，画像を利用することにより記憶可能性という点においてはすでに incentive が与えられていると考える．したがって阻害要因を知り，それを現状の手法とは別の手段で改善を試みるためにも，現時点での阻害要因をユーザ視点で把握することは意義のあることだと考える．

なお本研究における調査方法にはいくつかの問題があることは事実である．ランキングの生成という簡単だが抽象的な評価方法でアンケートを実施したため，得られたデータはどの設計要素が阻害要因であるかを具体的に特定するには不十分と言わざるをえない．また各システムの理解を被験者にゆだねすぎ，結果として本質的ではない要因による判断も調査結果に含まれているのは事実である．これらの問題は今後の調査では改善していく所存である．

5. おわりに

本論文では，画像を使用した認証を利用したことのないユーザが画像認証に対してどのような印象を持つのかをアンケートにより調査し，その結果について述べた．本調査により，画像認証の普及を阻害している可能性がある要因の一端を抽出できたと考える．この結果は，画像認証システムの設計やその改善において，機能実現のために手段を選択する際に回避すべき設計要素の指針として参照されることが期待され，画像認証に興味を持つ研究者やシステム設計者にとって有益な情報になると考えている．

また本実験によって，さらなる調査が必要と思われる興味深い結果が得られており，未利用者に対する追加調査を検討している．また論文 [10] にあるように，未利用者に対して実際にシステムを使用させ，使用前の印象がどのように変化するかについても，今後の課題としてその評価実験の実施を検討していきたいと考えている．

謝辞 本研究の実施に際して，授業実施の機会提供からその後の議論までさせて頂いた電気通信大学大学院 情報システム学研究科の小池英樹教授に感謝致します．

参 考 文 献

1) 高田哲司, 小池英樹: あわせ絵: 登録と通知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).
2) 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).
3) 増井俊之, IQ-Auth: 画像なぞなぞ認証システム, available from <http://iqauth.com/>, (accessed 2008-04-15)
4) Mnemonic Guard, (株) ニーモニックセキュリティ, available from <http://www.mneme.co.jp/>, (accessed 2008-04-15)
5) Rachna, D., and Adrian, P.: Deja Vu: A User Study Using Images for Authentication, *Proc. of the 9th USENIX Security Symposium*, USENIX, (2000). available from <http://www.usenix.org/events/sec2000/dhamija.html>, (accessed 2008-04-15)
6) visKey, SFR-Software, available from <http://www.sfr-software.de/cms/EN/pocketpc/viskey/>, (accessed 2008-04-15)
7) Leonardo, S. and Jean, C.B.: Graphical passwords, The Rutgers Scholar an electronic bulletin of Undergraduate Research, available from <http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm> (accessed 2008-04-15)
8) Luis, v.A., Manuel, B., John, L.: Telling Humans and Computer Apart Automatically, *Communication of the ACM*, Vol.47, No.2, pp.57-60 (2004)
9) Darren D., Fabian M., and Michael K. R.: On User Choice in Graphical Password Schemes, *13th USENIX Security Symposium*, pp.151-164, (2004)
10) Furkan, T., A.Ant, O. and Stephen H.H.: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords, *Proc. of the 2nd Symp. on Usable Privacy and Security (SOUPS'06)*, pp.56-66, (2006)
11) Rick, W. and Jeffrey K.M.: Incentive-Centered Design for Information Security, *1st USENIX Workshop on Hot Topics in Security*, pp.1-6, (2006)