Vol.2013-SPT-7 No.11
2013/11/11

“Exploring the Design Space of Graphical Passwords on Smartphones” の紹介

高橋 雅香[1,a)]　高田 哲司[1]

概要：本論文は，2013 年 7 月に英国で開催された Symposium on Usable Privacy and Security で発表された論文 “Exploring the Design Space of Graphical Passwords on Smartphones”[1] の研究内容を紹介する．

1. はじめに

Graphical password(図画利用認証) は文字列パスワードの欠点を克服しうる可能性を秘めており，また視覚情報の直接操作や選択の容易さからスマートフォン搭載のタッチスクリーンとの相性も良いと考えられる．しかし，Android 端末のパターンロックを除いて実際には普及していない．図画利用認証の設計要素は多数あり，それらが安全性，利便性および覗き見攻撃の可能性に影響を及ぼす．パスワードの記憶方法に限っても「完全記憶」「認識」「手がかり付き記憶」の３種類がある．このため，図画利用認証の評価結果は条件が異なることから単純比較できない．

紹介する論文では研究者や開発者を支援するため，図画利用認証の設計要素に関する解析を行う．その方法としては単一のプラットフォームを対象として５つに既存図画利用認証を実装して，デバイスの機能が設計にどのように影響するかを検証し，さらに被験者による評価実験を行うことで利便性と覗き見攻撃への影響を比較調査した．

2. デザイン領域

既存研究と一般的なガイドラインをスマートフォンの特徴と関連付けることによって，スマートフォンにおける図画利用認証のデザイン領域を位置付ける．デザイン領域は主にデザイン機能，パスワードの特徴，スマートフォンの能力の 3 つのグループに分けることが出来る．各々のグループは相互関係にあり，他のグループの能力を拡大あるいは制限することが可能な場合がある．

パスワードの特徴は安全性と利便性に大きく分けることができ，安全性対策を損なうことなく利便性を強化しなければならない．安全性面では理論的なパスワードの総数と実際のユーザが選択するパスワードの偏りの差が問題であり，デザイン機能において最適化を考慮しなければならない．同様にショルダーサーフィンも考慮するべき点である．利便性はログイン効率，ログイン成功率，パスワードを記憶出来るかどうかを測定基準として，既存のテキスト方式や PIN を上回るよう努めなければならない．

デザイン機能は認識メカニズムと情報表示方法，インタラクション方法によって決定することが出来る．認識メカニズムは，記憶力型，形認識型と手がかり記憶型に分類される．情報表示には格子構造の形，クリック方法，視覚的手がかり，非視覚的手がかりがある．また，インタラクション方法の選択もパスワードにおける重要な要素の一つであり，理論的なパスワード領域を増やすためにマルチタッチが用いられることもある．

スマートフォンや使用者の能力によって，デザイン機能が制限される場合がある．主な要因は並列可能なタッチ点の数などの入力能力，スクリーンや振動モーターなどの出力能力，使用環境，手や指の大きさや癖によるタッチ操作，使用者の視力などである．

3. デザイン領域の実行

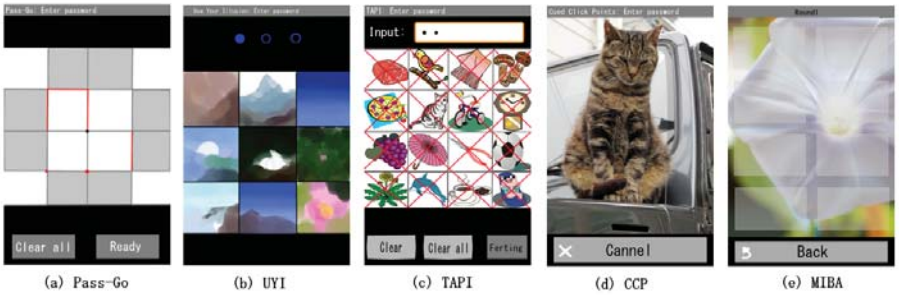
デザイン領域がどのようにスマートフォンの能力に影響を受けるかを理解するため，既存の５つの図画利用認証方式を，同じプラットフォームで実行した．

3.1 各方式の特徴

Pass-Go は，図 1a のように格子状の面の交点から交点へ線を引いて繋ぐことが出来る．点と線をつなぐ順番を正しく描かなければ認証出来ない．

Use Your Illusion(UYI) は認識ベースの方式である．鍵となる写真をおとり写真の中から選んでいく．ただし，ショルダーサーフィン対策のため，ログインの際は図 1b のように歪曲画像のみを見る．

[1] 電気通信大学
The University of Electro-Communications
[a)] m.takahashi@uec.ac.jp



(a) Pass-Go (b) UYI (c) TAPI (d) CCP (e) MIBA

図 1 実装された図画利用認証方式

Touchscreen Auth. using Partitioned Images(TAPI) は認識ベースと手がかり記憶の複合型である．図 1c に示すように，4×4 のアイコンを更に 1 つのアイコンにつき 4 分割を行っている．ユーザは正しいアイコンの正しい部分を選択しなければならない．

Cued Click Points(CCP) は手がかり記憶方式の規範的な例である．ユーザが点を自由に選ぶことが出来る画像を図 1d のように表示する．パスワード長の一連のクリックからパスワードは成る．

Multitouch Image Based Authentication(MIBA) は CCP に類似しており，最高 4 つの点のマルチタッチを用いる．図 1e のように，複数の指でクリック点を選ぶために，半透明の 2×4 のグリッドで覆われている．

4. 利便性実験

60 人の被験者を，PIN 方式含め 6 つのグループに分けて実験を行った．実験に用いるパスワードは 42bit と 14bit で，これはそれぞれテキストパスワード 7 桁と PIN4 桁に相当する．

4.1 入力時間とログイン成功率

bit 別にログイン成功率と平均入力時間を測った．入力時間は UYI が 42bit で 21.7(s) と最も長かった．ランダム配置の歪曲画像では，鍵を見つけるのが難しいからである．Pass-Go は両方のパスワード長で最も効率的だった．

普段から使用している被験者が存在したため，PIN はログイン成功率が最も高く 14bit で 100%となった．全体的にパスワードが長いほど成功率は低くなるが，TAPI のみ 14bit より 42bit の方が高い．MIBA と CCP は成功率が低く，1 枚の画像で認証する場合，間違いを戻す機能をつけても効果がないことを示唆している．

4.2 ユーザ満足度

4 項目を 7 段階の数値で算出する PSSUQ を用いて，各々の方式のユーザ満足度を測った．入力時間と成功率に有意差があるにも関わらず，全ての中央値は 5.44-6.8 の間にあったため，分散には有意差が見られなかった．ただし，各被験者は 1 つの方式しか実験していないため，個人間での比較ではない点は注意しなければならない．

5. ショルダーサーフィン実験

被験者が観測者としてショルダーサーフィンした場合と，ビデオで記録した場合で実験し，ショルダーサーフィン成功率を測った．14bit においては，CCP と TAPI が最小成功率であった．ビデオでは画面を仔細に認識するのが難しいため，成功率はほとんどの場合において低かった．

6. 議論

解析から得られたガイドラインは以下の通りである．1) 「手がかり記憶」と「認識手法」は安全性と利便性のバランスが良い．2) 選択対象は利便性が確保される範囲において小さい方が良い．3) 表示項目をランダムに配置するのは安全性と利便性の双方において望ましくない．4) 表示項目の時空間的配置法は利便性が維持されるようにすべきである．5) 手がかりを変更することは手がかりを固定するよりも安全性，利便性の点で望ましいという証拠はない．6) パスワードが長いほど覗き見攻撃に対して安全である． 7) 格子の視認性は利便性 (入力時間) の改善に寄与する．

7. 結論

紹介論文では，スマートフォンにおける図画利用認証の設計空間を分析し，デザイン領域での関係について議論した．そして，５種の認証手法を単一端末を対象として実装することにより，分析結果が今後の設計指標として十分な網羅性を持っているかを検証した．更に利便性と覗き見攻撃への脆弱性について被験者による評価を行い，どの設計要素と要素間の関係が安全性と利便性の双方を改善しうる要素かを検証した．

今後は今回の分析で評価した設計要素以外の要素も検討対象に加えて検討を進めるといった課題がある．

参考文献

[1] Schaub F., Walch M., Knings B, Weber M. :Exploring the Design Space of Graphical Passwords on Smartphones. Proc. of the 9th Symp. on Usable Privacy and Security (SOUPS'13), Article No.11, (2013).