Twitter を用いた携帯端末における個人認証の多要素化に関する研究

発表者: 総合情報学科 セキュリティ情報学 コース 学籍番号 1010086 高浪 悟
指導教員: 高田 哲司 准教授

1 はじめに

高性能な携帯端末の普及 [1] により，個人や決済にかかわる重要な情報を持ち歩くことが一般化しつつあり，警視庁もスマートフォンの電話帳データや位置情報などを不正に送信するアプリケーションソフトウェア (以下，アプリと略す) への注意喚起を行っている [2].

Apple 社が自社の製品である iPhone 5S に指紋認証機能を搭載したり，通常のスクリーンロックの多要素認証化を行う Hidden Lock[3] やアプリの起動などに対しても個別にロックを設定可能な AppLock[4] 等のアプリが配布されるなど，より多くの場面で個人認証の強化をはかる動きがある．

携帯端末におけるロック解除や，金融や Web サービスの多要素認証では，例えばハードウェアトークンを用いた所有物認証など，知識認証以外の手法を導入する例が多くみられるが，本研究では，ユーザからみた手軽さやサービスプロバイダが負担するコストなどの面から，知識認証を複数種類組み合わせる認証の多要素化手法を提案する．多要素認証を導入すれば当然ながらユーザの負担は増えるが，その負担増を最低限にするため，新たな操作法を習得する必要がなく，秘密情報の生成/記憶負担にも配慮した認証手法を考案する．

2 関連手法

携帯端末における個人認証を強化する手法としては，Google の開発している携帯端末向けプラットフォームである Android では第 1 章で述べた AppLock[4] や生体認証を利用できる PassBoard[5] などが存在する．

ライフログや SNS を認証に用いる手法に関して，西垣ら [6] は，ユーザの生活履歴を用いて認証を行う手法を提案し，そのプロトタイプとして E メールを用いたシステムの構築と実験を行った．E メールによる認証は，「最近のメールかどうか」をユーザに回答させるというプロセスで行われた．その際，人間の記憶の曖昧性を取り除くための手法として，最近と過去どちらともいえないような期間のメールを利用しない，例えば「8 日前から 29 日前までのメールは質問の中に出てきません」と明示することでユーザが直感的に回答を行えるようにした．また，Nemoto ら [7] は，Twitter のダイレクトメッセージ[*1](DM) 機能を用いて，定期的に質問を投げかけることでその回答を秘密情報とし，認証を行うシステムを提案した．質問の内容は「2 月 15 日の昼食は？」といった文面で構築され，Twitter のダイレクトメッセージ機能により送信され，回答も同機能を用いて行う．

3 提案システム

第 1 章での議論を基に，携帯端末の個人認証強化を目的とした，以下の特徴を持つ個人認証手法を実装した．

- 携帯端末の画面ロックにおける個人認証を想定する．既存のシステムは PIN による 1 要素認証だが，これに提案する認証を追加して 2 要素認証とする
- 秘密情報は，利用者が既知であるライフログや SNS の情報として Twitter のツイートを利用する
- 認証操作は回答選択方式で，既知の操作方法と同一にする

3.1 認証操作

本システムでは認証のために新たな操作を覚える負担を考慮し，認証操作に既存の携帯端末向け OS で既に実装されているロック画面中の通知機能を利用する際の操作と同等の操作で認証操作が可能なユーザインターフェイス (UI) を iOS アプリとして実装した．

通知の表示画面を模した認証画面 (図 1 左) では，10 個のツイートの本文と，当てはまるものがなかった場合に選択する「No match」の 11 つの候補を表示している．その中から，ユーザが正解だと判断した回答を選択すると PIN 入力画面に遷移する．

PIN 入力画面 (図 1 右) は既存の UI と同一であり，入力確定後に認証結果が表示される．両者の回答が共に正解であれば、認証に成功する仕組みとなっている．

3.2 秘密情報の設定

本提案では 2 種類 3 方法の秘密情報を検討し，実装した．1 つは既存の認証と同様の固定秘密であり，もう 1 つは規則を秘密情報とする可変秘密である．可変秘密の方法を採用した理由は，定期的な秘密情報の変更を能動的に行う必要が低減されるからである．

それぞれの秘密情報の設定方法は以下の通りである．

3.2.1 Auto Mode Type Term

可変秘密の 1 つであり，特定の期間を秘密とする手法である．つまり秘密である特定期間につぶやかれたツイートが秘密情報となる．期間の指定方法は開始する時期と期間 (例: 1 週間前から 3 日間) になる．設定時もしくは前回の認証時から新しく投稿されたツイートも秘密情報の候補として含まれ，ツイートを選択した後は従来の PIN 認証との比較のため 4 桁の PIN を入力する．

3.2.2 Auto Mode Type Cycle

可変秘密のもう 1 つの提案であり，特定期間を秘密とする点では前述の手法と同じであるが，秘密情報の指定は曜日と時間 (例: 水曜日の 23 時台) となる．新しく投稿されたツイートの扱いと認証の手順は Auto Mode Type Term に準ずる．

3.2.3 Manual Mode

利用者は、最新ツイート 200 件の中から、任意の 1 ツイートを秘密情報として選択する．不正解となるツイートはそれ以外の 199 件からランダムに抽出される．

4 利用可能性に関する被験者実験

提案手法の利用可能性について被験者により評価実験を行った．実験は提案 3 手法の他に比較対象として 5 桁の暗証番号認証を加えた 4 種類で実施した．各認証手法は 8 日間で 4 回の認証を

[*1] 特定のユーザ宛に，一対一で送信された文章のこと．閲覧可能な人物は，自分と相手のみである．

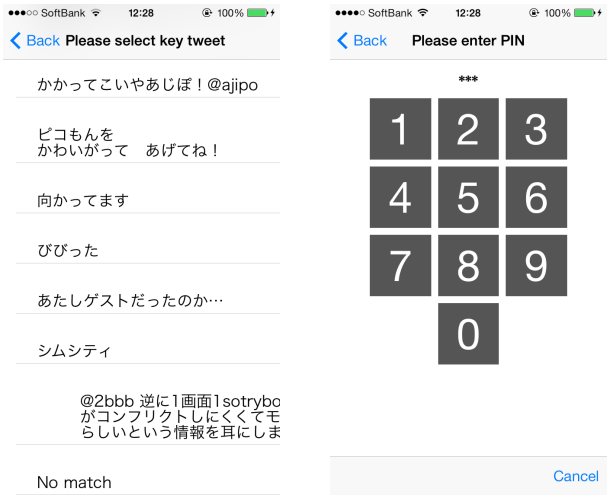

図 1　2 種類の認証操作画面

実施させ，認証成否と認証時間を測定した．被験者は 15 名で性別ならびに年齢構成は表 1 の通りである．また，4 種の評価実験のうち 2 種の実験を終了した時点で中間アンケートを，全て終了した後に最終アンケートを実施した．実験結果は表 2 に示す．

表 1　被験者の属性分布

	男性	女性
20 代	10 人	1 人
30 代	1 人	2 人
40 代	1 人	-

表 2　各手法における認証成功率と認証時間

手法名	認証成功率 (%)	認証時間 (秒)
Auto Mode Type Term	51.79	22.14
Auto Mode Type Cycle	27.59	22.95
Manual Mode	94.12	10.74
PIN Mode	94.34	2.56

5　考察

Manual Mode の認証時間は PIN Mode の 4 倍程度かかっており，特に一日に何度も認証を行う可能性の高い携帯端末では，利便性の面において改善が必要だと考えられる．しかしながら，アンケートによる比較では，使いやすさと憶えやすさ両方の項目で，Manual Mode が 4 パターン中最も優れているとした被験者が多かったことと，「認証にかかる時間はどのように感じましたか？」の問いに対する被験者の主観による評価は PIN と Manual で有意差がみられなかったことから，ユーザにとっては 5 桁の暗証番号と同程度の負荷，つまり安全性を強化するために「1 種類の秘密情報で秘密空間を拡大する」のと，「2 種類の秘密情報 (PIN+ ツイートによる 11 選択) を利用して安全性を強化」するのとで利用者が感じる負担は同程度だと言うことがわかった．

自動で設定する 2 手法 (Auto Mode Type Term と Auto Mode Type Cycle) では，PIN 認証と比べ大きく認証成功率が劣っているが，これはアンケートの内容から「設定情報は覚えているがそれに当てはまるツイートを選べない」という問題によるものであるといえる．この問題に対する改善策として，既存手法 [6] で対策されているのと同様に，独立した一つの情報，本システムの場合は 1 ツイートに対して 2-4 択で正解の選択肢を答えさせ，それを複数回繰り返すという方法が考えられる．既存手法ではこれに加え，曖昧な記憶による認証の失敗を防ぐため，はっきりと覚えている情報のみを認証に用いた．この 2 手法を導入することで，Auto Mode による秘密設定における認証成功率の向上が可能になると考える．自動で設定する 2 手法では，定期的な秘密情報の変更を能動的に行う必要が低減されることや，時間経過によるエントロピの増加などの利点が考えられたが，今後はそれらを活かすために認証成功率を上昇させることが最優先であると考えている．

6　おわりに

本研究では，現在の携帯端末の普及と情報の集約に伴う個人認証強化の必要性を議論し，知識認証の多重化による多要素認証を提案した．その際，既存の知識と操作を用いてユーザの負担を減らすべく，ライフログや SNS の情報を認証に使うことの有用性などを検討し，Twitter の情報を用いた携帯端末向け個人認証の多要素化手法の提案とプロトタイプシステムの実装を行った．また，実装したシステムを用いて被験者実験を行い，利用可能性について評価を実施した．

参考文献

[1] IDC Japan.　国内モバイル／クライアントコンピューティング機器家庭ユーザー利用実態調査結果を発表．入手先〈http://www.idcjapan.co.jp/Press/Current/20131003Apr.html〉（参照 2013-01-14）．

[2] スマートフォンを利用している方へ：警視庁.　入手先〈http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku414.htm〉（参照 2014-02-02）．

[3] Hidden Lock. 入手先〈https://play.google.com/store/apps/details?id=tv.marinelli.android.HiddenLock〉（参照 2014-02-02）．

[4] AppLock.　入手先〈https://play.google.com/store/apps/details?id=com.domobile.applock〉（参照 2014-02-02）．

[5] PASSBAN.　入手先〈http://www.passban.com/〉（参照 2014-01-25）．

[6] 西垣 正勝 and 小池 誠. ユーザの生活履歴を用いた認証方式：電子メール履歴認証システムネットワークセキュリティ. **情報処理学会論文誌**, 47(3):945–956, mar 2006.

[7] Tomofumi Nemoto, Kyohei Furukawa, and Manabu Okamoto. Poster: Knowledge-Based Authentication using Twitter. Symposium On Usable Privacy and Security 2011, 2011.