3W-04

スマートフォンにおけるアプリの利用時間を用いたフォールバック認証手法の検討

安齊将之　小倉加奈代　ベット B. ビスタ　高田豊雄
岩手県立大学　　ソフトウェア情報学部

1.はじめに

フォールバック認証とは，認証情報を忘れ，認証を繰り返し間違えた際の代替認証方式のことである．認証情報を忘れた場合，ロックを解除するために，バックアップから復元する，過去に同期した PC を利用して初期化することで対処できるが，別の端末が必要であるという利用上の問題がある．また，代表的なフォールバック認証の一種である「秘密の質問」は，利用機会が減多にないため，いざという時，ユーザが解答を思い出せない可能性がある．逆に思い出しやすい質問を設定すると，家族や友人，知人に推測されやすく，安全性に問題がある．

本研究では，前述のフォールバック認証における利用上の問題と安全性の問題を解決するため，ユーザが所持する端末上で，アプリの稼働時間のようなユーザしか知りえない情報を利用したフォールバック認証手法を提案し，その有用性および，安全性を評価する．

2.関連研究

Hang et al[1]では，スマートフォンにインストールされているアプリ情報を用いた質問による認証方法を検討した．この認証方式では，ユーザは，所有端末を対象とした「このアプリはインストールされていますか」の質問に「YES/NO」の 2 択で回答することで認証する．出題するアプリは端末にインストールされているアプリと Google Play Store で取得した 50 個のアプリから無作為に選び取ったアプリ（0～50 個）の総数（プリインストールアプリは含まない）で質問を生成する．この研究における問題点は，アプリのインストール数が極端に少ない場合，十分な質問を生成することが難しいこと，類似のアプリが出題された場合，片方を YES，もう片方を NO にし，確率を絞ることが容易であること，Facebook などの人気アプリが質問に出てきた場合，多くのユーザが YES と回答すると予想されることである．

3.提案手法

本研究では，Hang et.al[1]が利用したアプリのインストール有無に関する質問に，アプリの人気度を考慮し質問を作成することと，アプリの稼働時間に関する質問を追加することで攻撃者の認証成功確率を下げることを目標とする．本提案は，アプリの稼働時間という端末の所有者のみが知り得る情報を利用することにより，攻撃者にとっては回答が難しく，ユーザにとっては回答しやすくなるという著者の推測に基づくものである．本提案方式による認証は，図 1 のとおり，アプリのインストール有無に関する質問の認証に成功し，次にアプリの稼働時間に関する質問の認証に成功することで最終的に認証成功となる．次節よりそれぞれの質問認証について詳細に説明する．

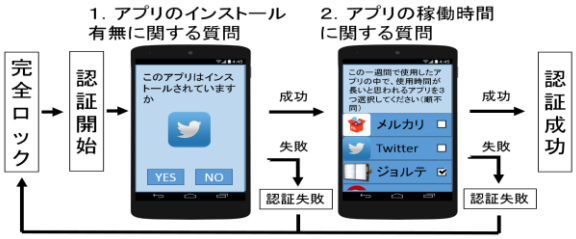

図 1　認証の流れ

3.1 アプリのインストール有無に関する質問認証

本認証では，ユーザは，「このアプリはインストールされていますか」という質問に回答する．ユーザの所有する端末にインストールされているアプリと，人気アプリランキング[2]から選んだ 50 個のアプリの総数から 40 個ランダムに選び取り，質問を生成する．40 問中 35 問以上正解で認証成功となる．

3.2 アプリの利用時間に関する質問認証

本認証では，ユーザは，「この一週間で利用したアプリの中で最も利用したと思われるものを 3 つ選択してください(順不同)」という質問に回答する．出題する不正解のアプリはインストールされていない前節と同様の人気アプリとインストー

A Study on Fallback Authentication Method Using Application Time on Smartphones
Masayuki Anzai, Ogura Kanayo, Bhed Bahadur Bista and Takata Toyoo
Faculty of Software and Information Science, Iwate Prefectural University

ルされているが，この 1 週間で 1 分以下しか利用されていないアプリである．アプリがバックグラウンドで稼働している場合は使用時間としてカウントされない．出題するアプリは正解のアプリを含めて 30 個である.3 つ全て正解した場合に認証成功となる．

4.評価実験手続き

インストール有無に関する質問と利用時間に関する質問のユーザおよび攻撃者の認証成功確率を評価する．ユーザとしての認証試行には，情報系学部所属の大学生 11 名，攻撃者としての認証試行は，被験者の友人・知人である情報系学部所属の大学生 11 名が参加した．アプリの利用時間に関する質問は，出題アプリの利用時間の取得期間を 1 週間と 1 か月の 2 種類生成した．また，ユーザ，攻撃者ともに認証上限は 3 回までとした．実験終了後に，全被験者はアンケートに回答した．

5.評価実験結果

5.1 インストール有無に関する質問認証

ユーザ認証実験では，ほとんどの被験者が試行回数 1 回で認証に成功した．40 問中何問正解できたかの正解率は平均 93.1%であり，最少 87.5%，最大 100%であった．認証時間は平均 70.6 秒であった．攻撃認証実験では全員が試行回数 3 回以内に認証に成功することができなかった．正解率は平均 55.0%であり，最小 40%，最大 67.5%であった．証時間は平均 73.4 秒であった．認証時間が 1 分以上かかるが，アンケートでは「手間はかからない」という回答が多く，質問数は適切であると考えられる．

5.2 アプリ利用時間に関する質問

表 1 および表 2 に稼働時間の質問のユーザ認証と攻撃者認証実験結果を示す．利用時間の取得期間が 1 週間，1 か月両方とも結果は大きく変わらなかった．先行研究[1]は正解率が 63.8%であった。この質問を追加すると，正解率はインストール有無の質問が 55%，稼働時間の質問が 18%であることから，全体の正解率は 10%となる．従って，攻撃者の認証成功率が下がったと言える．

回答内容を分析した結果，LINE などの SNS アプリが高頻度で正解アプリであることがわかった．多くの攻撃者はこれらアプリを正解として選択していた．また，アンケートから，1 週間で使用するアプリの個数は最低でも 6 個という回答を得た．したがって，SNS アプリを除外するか，もしくは選択数を増やしても，十分な質問を生成できると考えられる．それにより、攻撃者に突破されにくくなることが見込める．さらに，攻撃者のアンケートでどのようにアプリを選んだかの理由について、「長時間使用すると推測できるアプリを正解として選択した．」と回答していた。したがって、不正解アプリとして，明らかに長時間使用していないアプリは除外する必要があると考える．加えて，利用時間の取得期間が 1 週間よりも 1 か月の場合に有名アプリが出てくる可能性が高く，取得期間を 1 週間とするのが適切であると考えられる．

表 1　ユーザ認証の結果

取得期間	成功者数	認証時間（平均）	試行回数（平均）
1 週間	9 人	39 秒	1.8 回
1 か月	8 人	32 秒	2 回

表 2　攻撃者認証の結果

取得期間	成功者数	認証時間（平均）	試行回数（平均）
1 週間	1 人	74.5 秒	2 回
1 か月	2 人	68.6 秒	1.5 回

7. まとめ

本稿では，フォールバック認証における利用上と安全性の問題を解決するため，ユーザが所持する端末上で，アプリの稼働時間のようなユーザしか知りえない情報を利用したフォールバック認証手法を提案し，その有用性および，安全性を検証した．その結果，インストール有無の質問に稼働時間の質問を追加することにより， セキュリティ強度を上げることが出来た．しかし、攻撃者に破られるケースが見られた．今後は，実験結果に基づき質問の出題内容を改善し、有用性と安全性の再検証する．

参考文献

[1]Hang, A.,De Luca, A., Zezschwitz, E.,Demmler,M. and Hussmann,H.: Locked Your Phone? Buy a New One? From Tales of Fallback Authentication on Smartphones to Actual Concepts. Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI'15) pp295-305,2015 (参照2017-12-11)

[2] Applive:アプリランキング,入手先 (https://android.app-liv.jp/ranking/)(参照2017-01-06)