SAS-2 を用いた複数アプリ起動による認証方法

1180373　別府若奈　【 セキュリティシステム研究室 】

1　はじめに

今日，スマホサービスの発達により，携帯端末においてもユーザが管理するパスワード総数が増えている．そのため，パスワード管理としてメモを残したり，Cookie を保存したりする人も増加傾向にある．しかし，それらの方法では気軽に部屋を探索でき，端末を無断使用できる身内からの攻撃を防ぐことはできない．加えて身内の攻撃者は，パスワード認証の代替として注目されている生体認証においても指紋など生体情報の窃盗が容易であり，認証中に覗き見しても不審に思われにくい特性を持つ．

そこで本稿では，毎回認証を必要とする口座確認アプリなどに対して上記の問題を解決するために，個人が端末にインストールしているアプリを用いた手法を提案し，評価を行った．

2　提案方式

提案方式では，アプリを複数起動してパスワードを生成し，そのパスワードを用いて SAS-2 認証を行っている．SAS-2 は認証毎に認証情報が変化するワンタイムパスワード方式である．

通常，端末にインストールされているアプリには，一意に識別するためのアプリ ID が備わっている．認証画面においてアプリ ID を，図 1 のように，起動させたアプリの順番で抜き取り，統合させたものをパスワードとして扱う．この方式では，パスワードとして覚えるのは文字列ではなくアプリの起動順番であるため，ユーザの負担が少ない．加えて，アプリの起動中に覗き見されても，認証行為だと気づかれにくいメリットがある．

しかし，アプリ ID は一意に設定されているため，このままでは複数の人間が同じパスワードを生成してしまう恐れがある．そこで SAS-2 を適用し，乱数等を用いて個人の認証情報へと変化させる．SAS-2 を用いることで，リソースが限られたデバイスでも快適な動作ができ，通信路の情報が盗まれても次回の認証に必要な情報を取得できないようになっている [1].

3　評価

日本人は 100 個以上のアプリをインストールしている場合が多く [2]，以下では端末にインストールされているアプリ総数が 100 個だと仮定して提案方式の性能を評価した．表 1 は，起動アプリ数ごとのパスワードとして考えられる全ての組み合わせ総数，提案方式を実装した時において計測した認証動作の時間を示している．

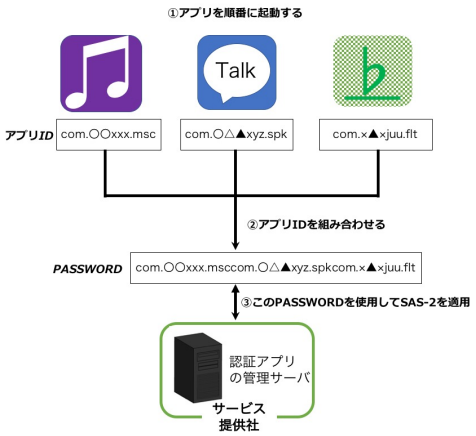

図 1　提案方式の概要図

表 1　起動アプリ数毎の性能

起動アプリ数 [個]	2	3	4
組み合わせ総数 [通り]	9,900	97 万	9,400 万
1 回の認証時間 [s]	12.91	17.42	26.63

提案方式の認証に使用するアプリが 2 種類の場合，その総数は 9,900 通りに及ぶ．そのため，偶然認証に成功する可能性は限りなく低いと考えられる．また表 1 より，使用するアプリ数が最も少ない 2 種類ですら，総当たりには約 30 時間必要とされる．したがって，端末を無断使用されても認証を突破する前に，端末の持ち主自身が異変に気付く時間が十分確保されているといえる．

4　まとめ

本稿では，ワンタイムパスワード認証方式 SAS-2 を用いて複数アプリ起動によるパスワード生成方式を提案した．本方式は個人が所有するアプリを自由に組み合わせてパスワードとすることができ，認証行為だと気づかれにくく，偶然の一致で認証成功する可能性は限りなく低いことが分かった．

参考文献

[1] 武政理恵, “ SAS-2 を用いた貸与型電子錠システムの提案 ”, 平成 26 年度　高知工科大学卒業論文, 2014.

[2] appllio, “ 日本人のアプリ所持数は世界一、1 人あたり平均 100 本以上をインストール—— App Annie 調査 ”, http://appllio.com/20170512-9129-app-install-no1-japan-app-annie-research, 2017 年 12 月 27 日閲覧.