ワンタイムパスワードによるパターン認証を用いたパスワードマネージャの提案

1180338　島田 憲吾　【 セキュリティシステム研究室 】

1　はじめに

近年, Web サービスの利用者が増加しており, ID・パスワードの使い回しが問題になっている. パスワードマネージャ(以下 PM) は複数の Web サービスの ID・パスワードを 1 つのマスターパスワードで集中管理するシステムであるが, 一般的な PM では安全な長さのパスワードを記憶しなければならないため, ユーザの負担が大きくなる問題がある. 既存方式 [1] では, パターンの記憶と証明書の所持の 2 要素認証を行うことで, ユーザの負担を軽減している. しかし, 全ての通信に安全な通信路を使用し、通信を暗号化しているため, 処理負荷が大きくなる問題がある. また, 複数の端末で PM を利用することができず利便性が低い. 本研究はパターン認証とワンタイムパスワードを用いて, 通信の処理負荷を軽減した認証方式を提案する. 加えて複数端末の利用を可能にすることで, 安全性と利便性を向上する.

2　提案方式

2.1　パターン認証

パターン認証とは, マスとマスをドラッグで繋ぎ合わせることでパターンを生成し, その順番の正誤で認証を行う方式である. パスワードは 12 桁以上の文字列がセキュリティレベルで推奨されており, 4 × 4 のマスで安全性を満たす [2]. 本研究では, ユーザが保存している乱数とサーバから送られてくる認証回数から生成した文字列を分割し, マス目に格納する. パターンで通ったマス目の文字列を連結し, ワンタイムなマスターパスワードを生成する.

2.2　提案方式のパスワードマネージャ

提案方式のフロー図を図 1 に示す. ユーザは提案方式を利用する際, ブラウザからアクセスを行う.

2.2.1　初回登録フェーズ

ユーザは ID と乱数 R を生成し保存する. 任意のパターンを入力する. その後, 安全な通信路を用いて ID・乱数 R・パターンをサーバに送信し, サーバは ID・乱数 R・パターンを保存しユーザを登録する.

2.2.2　利用フェーズ

ユーザはサーバに ID を送信し, サーバは ID に対応する認証回数 N を送り返す. ユーザは保存している乱数 R とサーバから受け取った認証回数 N からパターンのマス目の内部文字列の生成・格納を行いパターン認証を生成する. ユーザはパターンを入力し, マスターパスワード P をサーバに送信する. サーバも保存している乱数 R と認証回数からパターンのマス目の内部文字列の生成・格納を行い, 保存しているパターン通りにマスターパスワード P を生成する. 送られてきたマスターパスワード P とユーザ認証を行う.

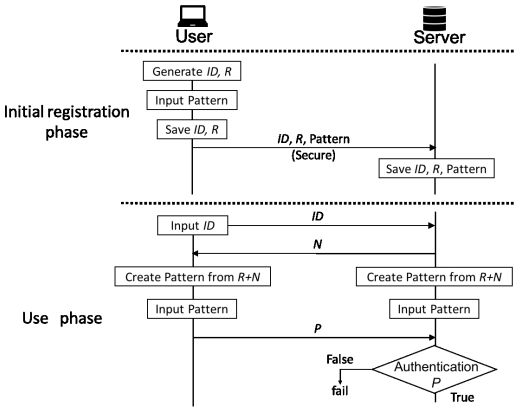

図 1　提案方式のフロー図

2.2.3　複数端末利用フェーズ

ユーザが未登録の端末 B で PM を利用する際, 認証済みの端末 A の画面に, ID と乱数 R を読み取ることができる QR コードを表示する. 端末 B は端末 A に表示した QR コードを QR リーダで読み取り, ID と乱数 R を端末 B に保存する. 端末 B は利用フェーズと同じ手順で PM を利用すことができる.

3　評価

通信に必要な暗号化回数と複数端末利用の比較評価を表 1 に示す. 既存方式は, 全ての通信に安全な通信路を使用し通信を暗号化しているため処理負荷が大きくなる問題と, 複数端末利用ができない問題がある. 提案方式は, 認証にワンタイムパスワードを使用することで, 認証に安全な通信路が必要なくなり, 処理負荷を軽減することができる. また, 複数端末の利用が可能になり, 利便性の向上できた.

表 1　性能比較評価表

	通信に必要な暗号化回数		複数端末利用
	初回登録	認証	
既存方式	4 回	4 回	不可
提案方式	1 回	0 回	可

4　まとめ

既存方式の認証情報をワンタイムパスワードにすることで, PM との通信の処理負荷を軽減することができた. また, 複数端末で利用が可能となり利便性も向上することができた. しかし, 共有情報 ID・乱数 R のユーザ管理方法について検討する必要がある.

参考文献

[1] 三本拓也, “パターン認証及びユーザ証明書を用いたパスワードマネージャの研究”, 2017/2/28

[2] 石黒司，福島和英，清本晋作，三宅優, “モバイル端末のロック解除向けパターン認証の安全性評価”, 電子情報通信学会技術研究報告，Vol.112，pp.273-278，2012.