パスワード管理システムに関する研究

1275095　青木 友志　【 セキュリティシステム研究室 】

A Study on Password Management Systems

1275095　Yuji Aoki　【 Security Systems Lab. 】

1　はじめに

Web サービスの発展に伴い, ユーザが管理する必要のある ID とパスワードの組数は増加している. 一方で, ユーザ自身が記憶しておける ID とパスワードの個数には限界があり全て記憶しておくことは現実的ではない. また, ID やパスワードをメモして持ち歩くこと等による漏洩のリスクも高まっている.

上記の対策として, ユーザの ID とパスワードを一元管理できるパスワード管理システムがある. パスワード管理システムにはさまざまな認証方式があるが, その多くはパスワード管理システム用の固定の ID とパスワードでログインする方式が採用されている. しかし, ID とパスワードが固定である場合, 通信を盗聴されることで ID とパスワードが漏洩しパスワード管理システムに預けてあるデータを取得することができてしまうため, なりすましや不正アクセスの可能性が生じる.

また, 近年では 1 人が複数の端末を所持している状況も増えてきており, 複数端末から 1 つの Web サービスを利用するケースも増加している. そのため, 複数端末認証が可能であることは必須といえる.

2　SAS

SAS は一方向性関数と排他的論理和によって構成されているワンタイムパスワード認証方式の 1 種である. SAS には, 中間者攻撃によるなりすましやリプレイアタックへの耐性を持つ SAS-2[1], サーバにある認証情報が漏洩した場合においても認証が可能である SAS-X, IoT デバイスにも適用可能にするために一方向性関数の回数を減らした SAS-L など複数のバージョンがある.

本研究では, ユーザ・サーバ共に処理能力が比較的高い点および, 通信を盗聴された場合においても認証情報が生成できないため認証時に安全な通信路が不要である点から, サーバにある認証情報が漏洩しても通信が可能である SAS-X を用いている.

3　既存方式

既存方式として渡邊の方式と高橋の方式がある. 渡邊の方式は SAS-X を改良してユーザ認証時に安全な通信路が不要かつ複数端末認証を可能にしている [2]. しかし, 新規端末の登録情報等の複数端末化する際に共有する情報に関しては安全な通信路が必要になる課題が挙げられている. 渡邊の方式における端末登録フェーズのシーケンス図を図 1 に示す. また, 渡邊の方式で用いている記法を以下にまとめる.

- N: 乱数
- ID, PW: ユーザの識別子, パスワード
- $H()$: 一方向性関数
- A: 新規端末 (端末 B) の初回認証情報
- SI: 共有情報
- G: ユーザの端末のグループの認証情報

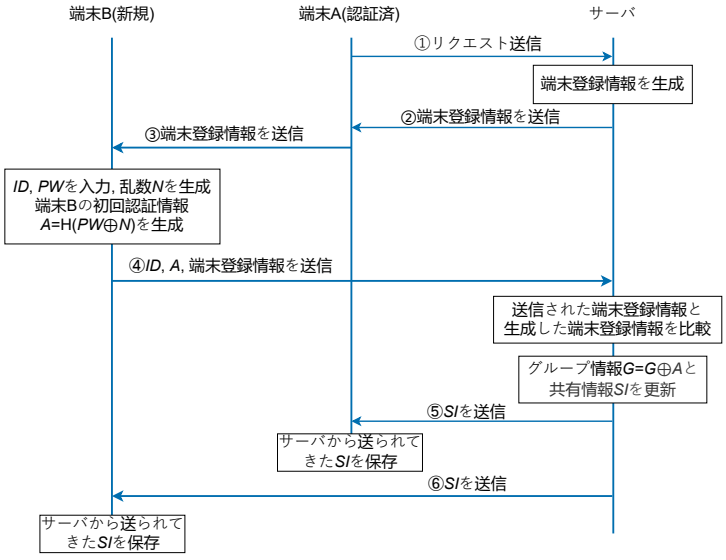

図 1　渡邊の方式: シーケンス図

高橋の方式では渡邊の方式で課題であった, 複数端末化の際の共有情報に安全な通信路が必要になる点を解決したている [3]. しかし, ユーザの端末ごとに認証情報を管理するためその管理コストが高い課題が挙げられている. 高橋の方式における新規端末登録フェーズのシーケンス図を図 2 に示す. また, 高橋の方式で用いている記法を以下にまとめる.

- K, L, V_1, N_i, N_{i+1}: 乱数
- ID, PW: ユーザの識別子, パスワード
- $H()$: 一方向性関数
- 端末 A の認証情報:
  $A_i=H(PW\oplus N_i)$, $F_i=H(A_i)$,
  $A_{i+1}=H(PW\oplus N_{i+1})$, $F_{i+1}=H(A_{i+1})$
  $\alpha_A=F_{i+1}\oplus F_i$, $\beta_A=F_{i+1}\oplus A_i$
- 端末 B の認証情報:
  $B_i=H(F_{i+1}\oplus K)$, $D_i=H(B_i)$,
  $B_{i+1}=H(PW\oplus V_1)$, $D_{i+1}=H(B_{i+1})$
  $\alpha_B=D_{i+1}\oplus D_i$, $\beta_B=D_{i+1}\oplus B_i$, $ID_B=ID\oplus L$

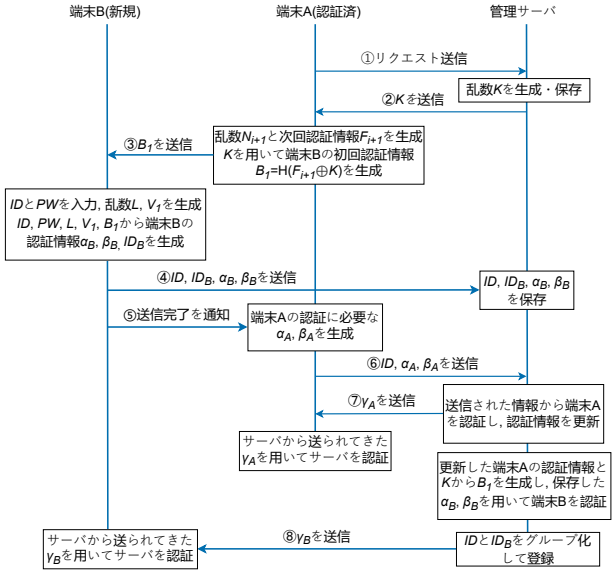

図 2　高橋の方式: シーケンス図

4　提案方式

本研究では, 既存方式の課題を解決した複数端末認証が可能かつワンタイムパスワードを効率的に利用可能なパスワード管理システムを提案する. 提案方式はユーザが利用するサービスの ID とパスワードの組をサーバのデータベースに登録する登録フェーズと, ユーザからの認証リクエストに応じてユーザの認証およびユーザが求める ID とパスワードの組を送信する利用フェーズの 2 フェーズから構成される. 利用フェーズのシーケンス図を図 3 に示す. また, 提案方式で用いている記法を以下にまとめる.

- R: 乱数
- n: インクリメント回数
- ID: サービスの識別子
- PW: ユーザとサーバの共有のパスワード
- $H()$: 一方向性関数
- ユーザの認証情報:
  $A_i=H(PW\oplus(R+n))$, $F_i=H(A_i)$,
  $A_{i+1}=H(PW\oplus(R+n+1))$, $F_{i+1}=H(A_{i+1})$
  $\alpha=F_{i+1}\oplus F_i$, $\beta=F_{i+1}\oplus A_i$

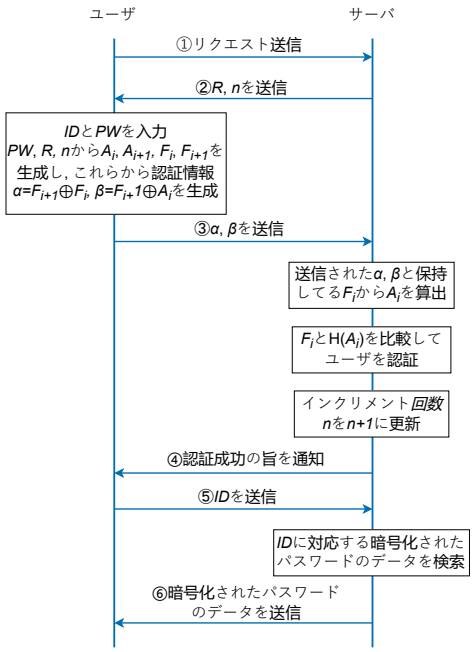

図 3　提案方式: シーケンス図

5　まとめ

本研究では, ワンタイムパスワードを効率よく利用可能かつ複数端末認証可能なパスワード管理システムを提案した. 今後の課題として, SAS-X の同期ずれを考慮したシステムの構築および, 乱数 R とインクリメント回数 n の送信方法の改良を行う必要性がある.

参考文献

[1] T.Tsuji,A.Shimizu. “A one-time password authentication method for low spec machines and on internet protocols”, IEICE Trans.Commun., vol.E87-B, no.6, pp.1594-1600, 2004.

[2] 渡邊 真悟, ”SAS-X を用いた複数端末認証可能なパスワード管理システムの提案”, 高知工科大学修士学位論文, 2017.

[3] 高橋 錬, ”サーバと端末間に安全な通信路を必要としない多端末認証可能なパスワード管理システムの提案”, 高知工科大学学士学位論文, 2018.