

パスワード管理システムに関する研究

1230286 青木 友志 【セキュリティシステム研究室】

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も増大している。しかし、個人が管理する ID とパスワードの組を全て記憶しておくのは困難である。また、パスワードをメモして持ち歩くこと等によるパスワードの漏洩のリスクも高まっている。

上記のリスクの対策として、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方式があるが、特に SSL を用いているものは導入・運用時にコストがかかる。この問題の解決策として SAS-2[1] を用いた方式が存在する。

しかし、上記の方式は複数端末認証が出来ないという問題点が挙げられる。複数端末から 1 つの Web サービスを利用する機会も増えており、複数端末認証できることは必須である。また、この問題を解決した既存方式では、各端末ごとに認証情報を管理するため認証情報の管理コストが高い問題点が挙げられる [2][3]。

そこで本研究では、SAS-2 よりも低負荷である SAS-L を用いて認証情報の管理コストが低く複数端末認証が可能なパスワード管理システムを提案する。

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 や、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。一方向性関数は演算数百回分に相当する処理負荷であるため、一方向性関数の回数がユーザ側で 0 回、サーバ側で 1 回である SAS-L は非常に処理負荷が小さい方式である。

3 提案方式

本研究では SAS-L を用いて、端末ごとの認証情報を保持する必要が無い複数端末認証が可能な方式を提案する。提案方式は登録フェーズと利用フェーズの 2 フェーズで構成される。登録フェーズでは、ユーザのパスワードの共有およびユーザが利用するサービスの ID とパスワードの組を登録し、利用フェーズでは、ユーザからの認証要求に応じてユーザが求める ID とパスワードの組を送信する。

利用フェーズのシーケンス図を図 1 に示す。

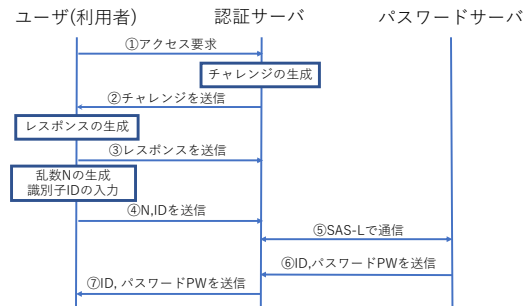


図 1 利用フェーズのシーケンス図

4 評価

渡邊の方式と高橋の方式、提案方式の評価を比較した結果を表 1 に示す。既存方式 2 種類と比べて、各端末ごとに認証情報を持つ必要がなくなったため、認証情報の管理コストが低くなった。

表 1 評価の結果

方式	安全な 通信路	パスワードの 安全性	導入 コスト	認証情報 管理コスト
渡邊の方式	必要	安全	高い	高い
高橋の方式	不要	安全	低い	高い
提案方式	不要	安全	低い	低い

5 まとめ

本研究では、SAS-L を用いて認証情報の管理コストが低く複数端末認証が可能なパスワード管理システムを提案した。また、2 種類の既存方式と比較し、提案方式が優位であることを示せた。

今後は、SAS-L の同期ずれを考慮したシステムの考案や、サーバ管理者の正当性を確認する機能の実装することが必要である。

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”, 高知工科大学修士学位論文, 2018.