SAS の同期ずれ解消時におけるなりすまし防止に関する研究

1130293　相川　由樹　【 清水研究室 】

1　はじめに

近年，個人情報漏洩の増加に伴い通信を安全に行えるワンタイムパスワード認証方式が注目されている [1]. SAS-2(Simple And Secure password authentication protocol ver 2)[2] を暗号鍵交換に応用した方式では，サーバ_クライアント間の通信経路遮断によって，認証情報が不一致となる問題が生じる. これを解決するために中原らが開発した方式では，同期問題発生時にサーバへ同じ情報を送信してしまう危険性がある [3]. 本研究では，同期ずれ発生時でも同じ情報を送信しない安全な同期問題解決手法の提案を行う.

2　なりすましを防ぐ認証方式

本研究では，同期ずれ発生時においても同じ情報を送信しない同期問題解決手法の提案を行う.

提案方式を SAS-2 に適用した場合の認証フェーズを図 1 に示す. 提案方式では，認証フェーズ開始時に乱数 Ni をクライアント側で生成し，次回用の認証情報 C を生成する．さらに C を用いてサーバに送信する α，β を生成する. これらの情報をサーバに送信する際に，通信路の遮断やサーバの不調等でサーバからの応答が一定時間無い場合，ユーザ側は同期ずれに対応した動作として Ni とは別の乱数 Ni' を生成し新しい次回用認証情報 C を生成する．サーバ側では同期ずれが発生した場合，同期ずれ確認に加えてなりすましの検証を行う. これにより，同期ずれが複数回発生した場合にも対応でき，同じ情報をサーバに送信することがなくなるため，認証の信頼性向上に繋がる.

2.1　実験方法

提案方式と従来方式をそれぞれ仮想マシンで実装した. それぞれの方式に対し，意図的に同期ずれを発生させ，実行同期ずれに対処できているかを検証する．さらに，通信路上でやりとりされたデータを再送し，第三者によるなりすましを再現する．また，提案方式と従来方式の認証ステップ数及び処理時間の差分を計測する.

2.2　実験結果，考察

検証の結果を表 1 に示す．検証の結果，提案手法は同期問題の解決に加えて，第三者によるなりすまし防止を行えることが実証できた．また，通常認証時においては一方向性関数の適用回数が従来手法と同等の回数で認証を行うことができた．同期ずれ発生時においても，従来方式と比較して同期ずれ 1 回あたり 2 ステップの増加で認証が行うことができる. 比較の結果，約 4 μ s の遅延で認証を行えるため，この遅延時間によって運営上に与える影響は少ないと言える.

表 1　提案手法と従来手法の比較

	同期対策	なりすまし	一方向性関数適用数	
			クライアント	サーバ
従来方式	100%	×	3	2
提案方式	100%	○	3	2

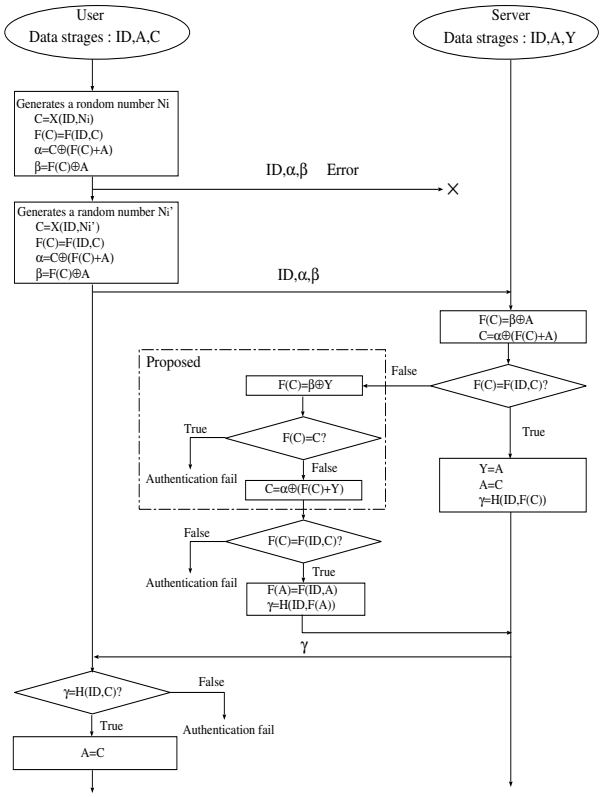

図 1　提案方式の認証フェーズ i 回目

3　おわりに

本研究では，SAS の同期ずれ解消時に発生する第三者からのなりすましを防止する手法について述べた．提案方式ではクライアント側サーバ側の情報保持量，認証ステップ数も通常認証時には同等の処理回数で行うことができた．今後の展望として，一方向性関数の適用回数が通信速度に及ぼす影響を検証していくことが挙げられる.

参考文献

[1]　警視庁,“平成 23 年度中の不正アクセス行為の発生状況等の公表について，”pp2，2012.

[2]　大垣文誉，小西竜也，辻貴介，清水明宏,“SAS を用いた Web 通信方式，”電子情報通信学会技術研究報告，OIS2003-6，vol.103，no.44，pp.31-35，2003.

[3]　中原知也，辻貴介，清水明宏,“SAS-2 認証方式の同期問題に関する検討，” 電子情報通信学会技術研究報告. OIS，vol.104，no.714， pp.83-87，2005.