セッション情報を不正に利用したなりすましを防止する方式に関する研究

1140349　田原　宏樹　【 清水研究室 】

1　はじめに

近年，多くの Web アプリケーションでセッション管理が用いられている [1]．セッション管理はセッション ID を持ちてユーザを管理するが，このセッション ID が悪意のあるユーザにわたってしまうとなりすましに利用される可能性がある [2]．そこで，本研究では，セッション情報を盗み取る攻撃でセッション情報が漏洩した場合でも，そのセッション情報の正当性を SAS-2[3] を用いて確かめることで，正規クライアントのみを判断できるシステムの提案，構築をおこなう．

2　なりすましを防止する認証方式

本研究では，SAS-2 を用いてセッション ID が漏洩した場合でも，正規クライアントのみを判断できるセッション管理の手法の提案・実装・速度測定をおこなう．提案方式の認証フェーズを図 1 に示す．従来，セッション ID が認証情報の役割を果たしていたものを，SAS-2 の認証情報（α，β）を用いて確かめることでセッション ID 漏洩に対するなりすましを防ぐことが可能となった．

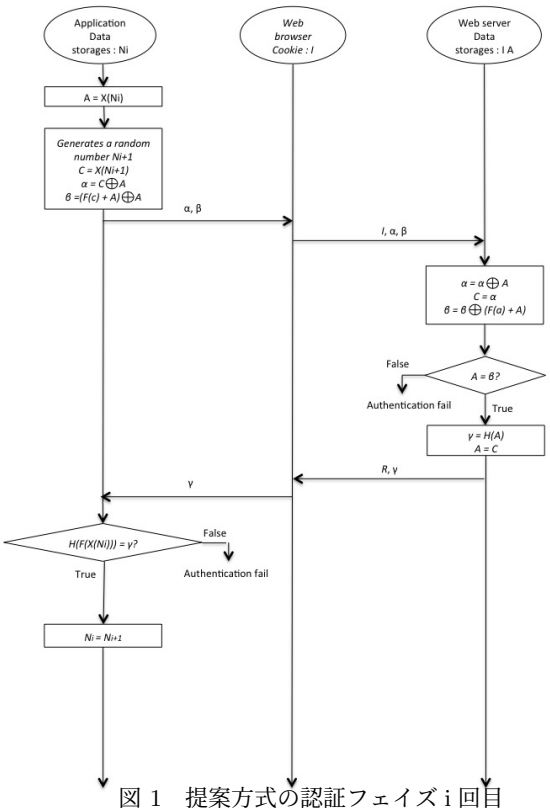

図 1　提案方式の認証フェイズ i 回目

2.1　実装

クライアント（java）・サーバ（PHP）の開発をおこなう．クライアント側のから HTTP 通信を行うには HttpURLConnection クラスを用いる．この API をブラウザとする．認証情報の送受信は，クライアントからサーバへの送信情報（A，α，β）は，POST を使用，サーバからクライアントへの送信情報（γ）は Cookie を使用する．認証情報の鍵長が 160bit，認証情報生成に用いたハッシュ関数が SHA 1，コンテンツには認証情報を鍵とした AES 暗号，アクセス毎に認証が行われる．

2.2　実験，考察

クライアント側で URL が読み込まれてから，表示が完了するまでの時間を測定する．提案方式と既存方式（SSL）との速度比較をおこなう．その結果を表 1 に示す．

	既存方式		提案方式	
	HTTP	SSL	SAS-2 なし	SAS-2 あり
速度（ms）	17.4	41.8	105.5	248.5
増加率（%）	140.2		135.5	
見込める速度減少（%）	4.7			

表 1　提案方式と既存方式の比較

現時点では SSL の方が 6 倍近く早い結果である．しかし，提案方式の SAS-2 なしは通常の HTTP 通信とみなすことが出来る，そのため，提案方式の HTTP 通信が既存方式の HTTP 通信同じ速度を出すことができれば，増加率の結果から（140.2-135.5）提案方式は SSL と比べて，4.7 %の速度削減が見込める結果となる．

3　おわりに

本研究では，SAS-2 を用いてセッション ID が漏洩した場合でも，正規クライアントのみを判断できるセッション管理の手法を述べた．今回はクライアント側のブラウザを java で開発したが，今後の課題として，は Google Chrome，Firefox 等のブラウザのアドオンでの開発をおこない．より一般的に使っていけるようにしていく工夫が必要である．

参考文献

[1] IPA, “ ソフトウェア等の脆弱性関連情報に関する届出状況, ” http://www.ipa.go.jp/security/vuln/report/vuln2012q3.html, 2012.

[2] IPA,“ 安全なウェブサイトの作り方　改正第 6 版, ” 独立法人 情報処理 推進機構, pp.22-28, 2012.

[3] 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.