IoT 環境へのセキュリティ方式実装に関する研究

1220299　稲村 圭悟　【 セキュリティシステム研究室 】

1　はじめに

近年のインターネットの進展に伴い，機械同士がインターネットに接続してデータをやりとりする IoT(Internet of Things) という利用形態が普及してきている．IoT においては，人が介在しない分，第 3 者によるデータの盗聴や改ざん等の脅威がより増加すると考えられる．このため，セキュリティ対策が必須となるが，接続される機器の処理能力に多様性があり，機器の処理能力に関わらず実装できるセキュリティ方式が求められる．

本研究室ではワンタイムパスワード認証方式 SAS の研究を進めている．SAS は，少ない計算量でワンタイムの認証情報を生成し認証を行い，その認証情報をシーズに生成する暗号鍵により暗号通信を行うセキュリティ方式を実現できる．

SAS の内，一方向性変換と排他的論理和を組み合わせて認証を実現する SAS-2 は，高速なワンタイムパスワード認証方式として，上位レイヤにおけるユーザの資格認証，ならびに下位レイヤにおいて情報送信単位毎に異なる鍵で暗号通信を行う方式として，無線 LAN 等のセキュリティに実装されている．

さらに，本研究室では，SAS-2 よりさらに高速処理が可能な SAS-L を考案し有効性の検証を進めている．

本稿では，比較的処理能力の低い IoT ゲートウェイという機器に対して SAS-2 と SAS-L をそれぞれ実装し，プログラムサイズおよび処理時間を比較し，両方式の適用領域について考察する．

2　実装方式

2.1　SAS-2

SAS-2 は従来の鍵配送方式として利用される RSA と比較して処理負荷が極めて低いワンタイムパスワード認証方式である [1]．認証情報が認証を行う度に更新されるため，認証情報を鍵とした鍵配送方式としての利用が可能である．SAS-2 は相互認証を行わない場合，一方向性関数をユーザ側で 1 回，サーバ側で 2 回の適用で実現している．一方向性関数は演算数百回分の処理を行うため，処理負荷は高くなる．

2.2　SAS-L

SAS-L は，SAS-2 よりもさらに低負荷な鍵配送方式として利用できるため，センサ等の処理能力の低い機器への実装を想定した方式である [2]．また，鍵配送と相互認証を同時に実現している．SAS-L は一方向性関数をユーザ側で 0 回，サーバ側で 1 回の適用であるため，SAS-2 よりも軽量な方式である．

3　実装環境および性能比較結果

処理機能を有するセンサ等の IoT 機器が存在していないため，比較的処理能力の低い IoT ゲートウェイ (Armadillo 製 G3L モデル) をクライアント環境とし，汎用 PC をサーバ環境として実装実験を行った．

本実験では，クライアント環境において OS は Debian GNU/Linux 9(stretch) で開発言語を C 言語で実装した．各方式を実装した際のプログラムサイズを計測した．また各方式の認証および鍵共有までの処理を 10 回行い，処理時間を計測した．そのプログラムサイズと処理時間の平均を表 1 に示す．実装実験の結果，SAS-L は SAS-2 と比較して，プログラムサイズが約 40%小さく約 140 倍高速であった．

表 1　クライアント環境のプログラムサイズと平均処理時間

方式	プログラムサイズ [Byte]	平均処理時間 [ms]
SAS-2	7976	3.9207
SAS-L	4723	0.0281

4　まとめ

本稿では処理能力の低い IoT 機器である IoT ゲートウェイに対して SAS-2 および SAS-L を実装した．SAS-L は SAS-2 に比較して，小さいプログラムサイズで格段に高速処理で実現できることを確認した．今回はソフトウェアでの実装実験を行ったが，専用のハードウェアで実現した場合，SAS-L は極めて少ないゲート数でその機能を実現できるため，センサ等の単機能の IoT 機器へのセキュリティ機能の実装を可能とすることが期待できる．

今後，ハードウェアでの実現方式を評価することが課題である．

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] 太田 愛里，"IoT に適したワンタイムパスワード認証方式に関する研究 ”，高知工科大学修士学位論文，2017.