ワンタイムパスワード認証方式の実装と評価

1190297　稲留　亮太　【 セキュリティシステム研究室 】

1　はじめに

近年，IoT（Internet of Things）の発展が目覚ましい．産業や生活において生産性，利便性の向上が期待されるがこれまでより人とインターネットに接続された端末が密接になるため，意図しない不正操作やプライバシー問題などが懸念される．よって暗号化による安全な通信経路の確保が必須である．IoT 機器の特性上限られたリソースの中での処理が求められる．そこで暗号化の際の低負荷な鍵配送方式として IoT に適したワンタイムパスワード認証方式 (SAS-L)[1] が考案された．

そこで本稿では考案された認証方式を用いた IoT を想定した環境を構築する．その性能評価として処理速度，消費電力に着目し定量的な評価を行う．測定結果よりワンタイムパスワード認証方式 SAS-2，SAS-X と比較し考案された認証方式の有用性について検証する．

2　ワンタイムパスワード認証方式

2.1　SAS-2

SAS-2[2] は反射攻撃 (Replay Attack) や中間者攻撃 (Man-in-the -middle Attack) などによるなりすましに耐性のあるワンタイムパスワード認証方式である．クライアント，サーバー間で相互認証が行え鍵共有方式としても扱える．類似する認証方式に比べ一方向性関数の適用回数が少なく処理負荷が少ないが IoT 機器等の想定される処理能力では負荷がかかると言える．

2.2　SAS-X

SAS-X[3] はサーバー側，認証者による情報漏えいが起因となるなりすましに耐性があるワンタイムパスワード認証方式である．登録フェーズにて悪意ある第三者が初期登録情報を盗聴したとしても認証情報を生成することは不可能である．よって初回登録時に認証情報を完全に安全な経路を確保する必要がないと言える．SAS-2 と同様に一方向性関数の適用回数は少ないが IoT 機器等の想定される処理能力では負荷がかかると言える．

2.3　SAS-L

IoT に適した認証方式として一方向性関数を使用しない低負荷な方式かつ鍵配送方式としても扱うことができる．登録フェーズと認証フェーズに分かれて構成され，初回登録時は安全な経路で初回認証情報を共有する．登録フェーズ以降，認証フェーズでは認証及び鍵交換を繰り返す．

2.3.1　登録フェーズ

クライアントは自身の識別子 ID，パスワード S を入力し乱数 N_1，M_1 を生成し保存する．その後 ID，S，N_1 を用いて認証情報 $A = F(ID|S \oplus N_1)$ を算出し保存する．そして安全な通信路にて ID，A，M_1 を送信し，サーバーは受け取ったのちすべて保存する．

- F は，一方向性関数である．
  例として F(x,y) は x と y を結合した値に一方向性関数を適用することを表す．
- $\oplus$ は，排他的論理和演算子表す．

2.3.2　認証フェーズ

認証フェーズでは，認証情報を用いてユーザ，サーバー間で相互認証を行い，認証情報 A とマスク値 M_i を更新する．

3　実験

実験環境として，サーバーを想定した汎用 PC，IoT 機器を想定した超小型かつ安価な ARM コンピュータである Raspberry Pi Zero を利用する．また，各認証方式における乱数生成及び共通鍵生成などの暗号化処理の関数は OpenSSL を利用して簡易的に実装する．それぞれ登録フェーズが終了後，認証フェーズのリクエストから相互認証完了までを 1 回とし計 10 回の処理時間とその間の消費電力を測定する．消費電力の測定は簡易 USB 電圧・電流測定器を Raspberry Pi Zero と供給電源の間に用いる．

4　評価

登録フェーズにて入力する ID，パスワードは同じものとして実験を行う．測定された結果より，平均処理時間と平均消費電力を比較し評価する．

5　まとめ

本稿では，IoT に適したワンタイムパスワード認証方式を実装と他の認証方式との比較をし，有用性につて検証を行う．

参考文献

[1] 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”，平成 29 年度　高知工科大学修士学位論文，2017.

[2] T.Tsuji，A.Shimizu，“Simple And Secure password authentication protocol Ver.2 (SAS-2)”，IEICE Technical Reports，OIS2002-30，2002.

[3] T.Tsuji，T.Nakahara，A.Shimizu，“A one-time password authentication method”，IEICE Technical Reports，OIS200583，Jan．2006.