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

1205079　太田　愛里　【 セキュリティシステム研究室 】

A one time password authentication method applicable to secure IoT for communications

1205079　Eri　Ota　【 Security Systems Lab. 】

1　はじめに

近年, パソコン以外の物をインターネットに接続する IoT(Internet of Things) が発展してきている.IoT 機器には Web カメラや IC タグなどがある. 例えば Web カメラの通信が暗号化されずにやりとりされた場合, 他人に見られたくない画像が流出してしまうという事が考えられる. よって IoT 機器にも暗号化が必要であるが, 暗号化には鍵配送方式が必要である. 暗号化の為に使う鍵配送方式としてワンタイムパスワード認証方式 SAS-2(Simple And Secure password authentication protocol, ver.2) を使う方法が存在する [1]. しかし IC タグなどの処理能力の低い IoT 機器で利用する為には, 更に負荷の低い方法を考案する必要がある.
本稿では, 低処理能力の IoT 機器でも利用可能な鍵配送方式の提案を行う.

2　SAS-2

SAS-2 はワンタイムパスワード認証方式の一つで, 一方向性関数と排他的論理和によって構成されている. 認証の度に認証情報が更新される性質があり, 認証情報を鍵として使う事で鍵配送方式としても利用可能である. しかし IC タグなどの低処理能力の IoT 機器で利用することを考えた場合, 一方向性関数は普通の演算数百回分の処理を要する為処理負荷が高くなる.

3　提案方式

本稿では, 低処理能力の IoT 機器でも利用出来るように, 一方向性関数が不要で, 鍵配送方式としても使えるワンタイムパスワード認証方式を提案する. 提案方式は最初の一度だけ実行される登録フェイズと通信の度に行われる認証フェイズから構成される. 登録フェイズでは初回認証情報を安全に共有し, 認証フェイズでは認証及び鍵更新を行う.

3.1　登録フェイズ

ユーザ側は乱数 N_1, M_1を生成する.その後入力された ID, パスワード S, N_1を使って $A = F(ID \mid S \oplus N_1)$ を算出する.そして ID, A, M_1を安全なルートを用いてサーバへ送信し, サーバは受け取った ID, A, M_1を保存する.

3.2　認証フェイズ

提案方式の i 回目の認証フェイズを図 1 に示す. 認証フェイズでは, 認証情報を用いてユーザ, サーバ間で相互の認証を行い,認証情報 A, M_iを更新する.

4　評価

提案方式では, 前回の認証情報を記憶していた場合, サーバ側の処理が足し算などの普通の演算数回で済み, 一方向性関数が不要となる. 鍵配送方式として利用する場合, ユーザ側とサーバ側を逆にしても問題無い為,IoT 機器側にサーバ側を適用すれば処理能力の低い IoT 機器でも利用可能となる.

5　まとめ

本稿では, 低処理能力の IoT 機器でも利用出来るように, 一方向性関数が不要で普通の演算数回のみで利用可能な鍵配送方式としても使えるワンタイムパスワード認証方式を提案した. 今後は実際の IoT 機器への実装などが考えられる.

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.

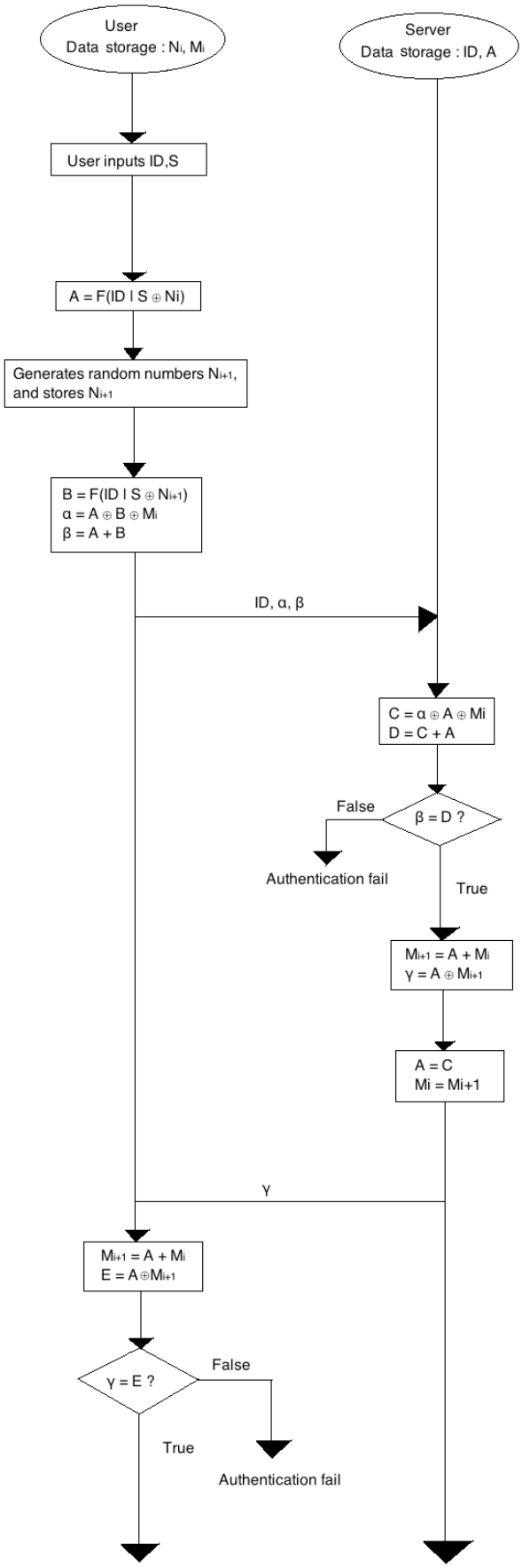

図 1　提案方式の認証フェイズ