2F-7　SAS型共有鍵暗号方式に関する研究

有信 勝弘† Manjula Sandirigama† 清水 明宏‡ 野田 松太郎†

†愛媛大学工学部 ‡高知工科大学情報システム工学科

1 はじめに

現代、様々な情報がデジタルデータとしてネットワークを通じて伝送され、利用されている。しかし、これらのデータが悪意を持つ第三者によって脅かされる危険性も高まっている。

このような危険の中に電子メールがあげられる。データの盗聴、データの改ざん、発信者のなりすまし等の危険性がある。このような危険からデータを守るための手段として、暗号技術の導入が必要とされる。

最近注目されつつあるのが携帯端末を用いた電子メールの暗号化である。現在、パソコン等を利用した電子メールの暗号化ツールが存在するが、公開鍵方式を使用しているため、メモリや処理能力に制限がある携帯端末には使用することができない。そのため、端末側の負荷が小さく、携帯端末での適用が可能なシステムが望まれる。

Sandirigama 等により提案されている Simple and Secure Password Authentication Protocol(SAS) を用いたメッセージ交換システム [1] は、ユーザ認証に従来方法より計算量の低い SAS を用い、暗号鍵共有方式が採用することにより計算負荷は少なく、携帯端末で用いられるようなシステムには適している。しかし、メッセージを交換する者が悪意を持っている場合、安全面における問題がある。本論では SAS を用いたデータ交換システムの問題点について指摘し、それを改善する方法について検討する。

2 SASを応用したメッセージ交換システム

Symmetric key cipher system based on SAS

Katsuhiro Arinobu†, Manjula Sandirigama†, Akihiro Shimizu‡, Matu-Taro Noda‡

† Department of Computer Science,Ehime University

‡ Kochi Institute of Technology

ここで用いられる記号の定義について始めに述べる。

- S_a, S_b: それぞれユーザ A,B のパスワード
- E: ハッシュ関数
- N_n: n 回目の認証に用いられる乱数
- //: 連結
- $E(X)$: X に一度ハッシュ関数を適用したハッシュ値
- $E^2(X)$: X に二度ハッシュ関数を適用したハッシュ値
- $A \rightarrow B$: A を B に送信する。

[1] で提案されたメッセージ交換システムでは、メッセージの暗号方式には暗号鍵共有方式を利用し、認証方式には SAS で用いられた方法を利用し、計算負荷が少ない手順で安全なメッセージ交換が実現できるよう提案されている。

メッセージの交換には、信頼されているセンタが発行する 2 つの値 X, Y が記憶されたプリペイドカードが用いられる。メッセージを交換する全てのユーザは、まず始めにそのカードを購入しておかなければならない。ここで、X はユーザ ID を表し、Y はカードを購入したユーザとセンタにしか分からない秘密の値を表す。

ユーザ B がユーザ A へメッセージを送信する場合、以下の手順で行われる。ユーザ A と B はカードを購入し、X_A, Y_A と X_B, Y_B をそれぞれ取得していると仮定する。

・初期値 $E^2(S_a//N_{0a})$, $E^2(S_b//N_{0b})$ の登録

1. ユーザ A : ユーザ B に対して X_B を要求する。
2. ユーザ B : $X_B \rightarrow$ ユーザ A
3. ユーザ A : $X_A, X_B, Y_A \oplus E^2(S_a//N_{0a}) \rightarrow$ センタ

4. センタ : Y_A を使って $E^2(S_a//N_{0a})$ を計算。Y_B を使って $Y_B \oplus E^2(S_a//N_{0a})$ を計算。
X_A,$Y_B \oplus E^2(S_a//N_{0a})$ → ユーザB
5. ユーザB : Y_B を使って $E^2(S_a//N_{0a})$ を計算。

以上の1から5の手順を、ユーザAとユーザBを入れ換えて行い、初期値 $E^2(S_b//N_{0b})$ の登録をユーザAで行う。

・ユーザ認証，メッセージの暗号化，復号化

1. ユーザA :
$E(S_a//N_{0a}) \oplus E^2(S_a//N_{0a})$ → ユーザB
$E^2(S_a//N_{1a}) \oplus E^2(S_a//N_{0a})$ → ユーザB
2. ユーザB : 初期値 $E^2(S_a//N_{0a})$ を用いて $E(S_a//N_{0a})$, $E^2(S_a//N_{1a})$ を得る。
3. ユーザB : $E(S_a//N_{0a})$ にハッシュ関数を適用し、得られた値と初期値 $E^2(S_a//N_{0a})$ が一致したら相手がユーザAであることが認証できる。認証が成功すれば初期値を $E^2(S_a//N_{1a})$ に更新する。この値が次の認証に使われる。
4. ユーザB : $E(S_a//N_{0a})$ を暗号鍵としてメッセージを暗号化。
$E(S_a//N_{0a})$[メッセージ] → ユーザA
5. ユーザA : $E(S_a//N_{0a})$ を使って復号化。

ここでの手順1,2,3の認証はSASで提案されている認証プロトコルを用いている。$E^2(S_b//N_{0b})$ はユーザAがユーザBにメッセージを送信する場合に使われる。

3 問題点と解決方法

このシステムでは、第三者からの危険性はないが、通信者が悪意をもった場合、初期値の登録において秘密データであるYを知ることができる。以下にその手順を示す。

1. 初期値の登録の3でユーザAからセンターに送られる $Y_A \oplus E^2(S_a//N_{0a})$ を通信相手であるユーザBが盗聴する。
2. ユーザB は初期値の登録の 5 により $E^2(S_a//N_{0a})$ を入手する。
3. ユーザBは盗聴したデータと自分がもっている $E^2(S_a//N_{0a})$ をXOR演算する。
$Y_A \oplus E^2(S_a//N_{0a}) \oplus E^2(S_a//N_{0a}) = Y_A$
4. これによりユーザBは Y_A を取得する。

この問題点を解決する方法を以下に示す。
初期値データの登録において
$Y_A \oplus E^2(S_a//N_{0a})$ を $E(M_A//Y_A) \oplus E^2(S_a//N_{0a})$ とする。M_A は乱数を表す。この M_A もセンターに送信し、ユーザBに送信することで同様に初期値を送信できる。このような考え方によると、初期値の登録は以下のように書き換えられる。

1. ユーザA : ユーザBに対して X_B を要求する。
2. ユーザB : X_B → ユーザA
3. ユーザA : X_A,X_B,M_A,$E(M_A//Y_A) \oplus E^2(S_a//N_{0a})$ → センタ
4. センタ : M_A,Y_A を使って $E(M_A//Y_A)$ を計算し、この値を使って $E^2(S_a//N_{0a})$ を計算. M_A,Y_B を使って $E(M_A//Y_B)$ を計算し、この値を使って $E(M_A//Y_B) \oplus E^2(S_a//N_{0a})$ を計算。
X_A,M_A,$E(M_A//Y_B) \oplus E^2(S_a//N_{0a})$
→ ユーザB
5. ユーザB : M_A,Y_B を使って $E(M_A//Y_B)$ を計算し、この値を使って $E^2(S_a//N_{0a})$ を計算。

こうすることにより、上述の手順によって盗聴したとしても $E(M_A//Y_A)$ しかわからない。しかしながらハッシュ関数は一方向性関数なのでこの値から Y_A を知ることは不可能である。

4 むすび

解決方法を用いることによってより安全なシステムを作成することができた。この方法によってハッシュ関数を適用する回数が増えるが、処理速度にはさほど影響はない。そのため、負荷が小さくかつ安全で、携帯端末への適用が可能なメールシステムの作成が可能となる。

参考文献

[1] M. Sandirigama, A. Shimizu and M.T. Noda : Simple and Secure Password Authentication Protocol (SAS),IEICE Trans.Comm.,(to be published)