

3ZC-05 秘密を分散管理する個人認証システムの開発

細畑幸伸 千石 靖 服部進実

金沢工業大学情報工学科

1. はじめに

コンピュータの利用の中で、個人認証は一般的な自衛の方法として、情報セキュリティ技術の一部として利用されてきた。とりわけネットワーク環境が大きく発展してきている現代では、非対人環境における本人認証の重要性が高まってきている。そこで、今回はこれまで研究されてきたシステムの利点をうまく融合させることにより、高速で安全性の高い個人認証システムの開発を目指すこととした。

2. 既存の個人認証システムとその欠点について

現在最も利用されている認証方式にパスワード方式がある。この方式は知識による認証であり簡単に行えるが、しかしパスワード入力時に盗み見されたり、簡単なフレーズではパスワードファイル内のハッシュ値の漏れから辞書攻撃されるなどの欠点がある。また持ち物による認証では IC カードなどがよく利用されている。しかしこれもカードの紛失や盗難などがあり、正当な権利を持たない者でも利用できてしまう危険性がある。さらに専用の読み取り機が必要でありコストがより高くつく。さらに身体的特徴による認証では、その値は固有のもの（指紋、音声など）であるが認証率やさらに特殊な読み取り機のコストの問題、またその普及率にも問題がある。

3. 解決への方策

以上のとおり、個人を認証するために使われるデータは知識、持ち物、身体的特徴が存在するが、研究の前提として既存の認証方式の欠点を補い、コストの面を考え携帯端末の利用をやめ、利用者が必要最低限の動作で認証手続きが行えるシステムの開発を考える。そのため一般的に多く利用されているパスワード方式を利用し、この欠点をなくすような認証システムの開発を目指す。

反面先ほど述べたようにこの方式では、パスワード入力時の盗み見（キーボード入力位置の把握）や簡単なフレーズではハッシュ値の漏れから辞書攻撃されるという欠点があった。そこでこの問題を解決する1つの方法として one-time password の利用を考えた。one-time password とは 1 回の認証手続きごとに秘密が変化するという構造的特徴を利用して認証を行うものであり、盗み見などに効果があると考えられるためである。さらに良い事に one-time password の構造として一方向性関数を利用するものがあり、この一方向性関数の利用は処理の高速化も期待できるため、うまく取り入れる方法は無いかと考えた。しかし一方で毎回変化する秘密を計算するために携帯端末の利用が必要となり、先ほど述べた研究の前提とは異なってしまうため one-time password のみの利用では問題点が残ってしまう。

A User Authentication System with Secret Sharing

Yukinobu Hosobata, Yasushi Sengoku and Shimmi Hattori

Information and Computer Engineering, Kanazawa Institute of Technology

7-1 Ohgigaoka Nonoichi Ishikawa 921-8501, Japan

4. 新しいシステムについて

そこでこの one-time password を利用した新しい認証システムを考えたとき、昨年開発された個人認証システム^[1]の欠点を補い利用できると気づいた。

昨年開発されたシステムとは、パスワードの検証を行う秘密情報をこれまでとは違い認証サーバ側ではなく暗号化を行ってフロッピーディスクに保存しておき、認証時の入力文字列と共に認証サーバに送り検証を行うというものである。これにより認証サーバから秘密が漏れることはありえないし、フロッピーディスク内の情報も暗号化を施してあり、こちらも秘密の漏れはない。入力文字列についても任意の文字列を前後に挟む（“任意の文字列＋秘密＋任意の文字列”）ことにより盗み見の防止を行っている。しかしこのシステムでは構成上クライアント PC に秘密を所持させないため暗号通信の部分で公開鍵暗号を利用しており、そのため処理速度が遅く 1～2 分かかってしまうという欠点があった。そこで今回の研究ではこの欠点を改良すべく、暗号化処理の高速化を目指し one-time password を利用し、さらに安全性の高い認証システムの開発を目指した。

5. 改良点

(1) 認証の高速化

既存のシステムでは公開鍵暗号を利用しており、これにより鍵生成に 1～2 分かかってしまう。そこで先ほどの one-time password の原理を利用することにした。具体的には、安全性を考慮し一方向性関数を逆順で利用して同期を取り、認証サーバ側とクライアント PC 側で毎回異なる共通の鍵を作る。次にこの鍵を用いて共通鍵暗号を利用し暗号通信を行う。これにより暗号化処理は格段に高速化し一瞬でのログインが可能となる。

(2) 安全性の向上

今回のシステムではクライアント PC 側に一方向性関数のシードなどの秘密情報があり、安全性の確保が求められるが、まず考えられる問題としてクライアント PC そのものがデッドコピーされる場合があるだろう。これはクライアント PC の IP アドレス等の確認を行うことによって、正規の端末であるかが確認でき、この問題は解決できると考えられる。しかしクライアント PC 側の一方向性関数などの秘密情報などが漏れてしまった時にこの情報が別のクライアント PC で利用されてしまう場合も考えられるが、この問題に対しては現在のところ秘密情報の難読化を行い、さらに一方向性関数のシードを定期的（99 回程度）に変更するという対策で解決できると考えている。

6. まとめ

以上のことにより、今回のシステムでは既存のシステムの、「盗み見の防止」「サーバ側からの秘密の漏れ防止」という利点を利用し、欠点であった暗号化処理のスピードを one-time password の原理を利用することにより解決した。さらに毎回変化する共通鍵により暗号化通信の安全性も向上されたことになる。

参考文献

- [1] 坂巻将史, 千石 靖, 服部進実: 新しいユーザ認証方式の開発とその評価, 1999 年暗号と情報セキュリティシンポジウム予稿集, pp.741-746 (1999)