バイオメトリクスのUNIXログイン認証への応用

古川 英雄† 塙 敏博‡

東京工科大学 工学部 情報工学科§

1 はじめに

従来, コンピュータシステムへのログインには, 主にパスワード認証が用いられてきた. これは本人だけがパスワードを知っていることを前提にした認証方法であり, 以下のような問題があった.

- パスワードを推測され, アカウントを不正に利用される.
- 本人がパスワードを忘れる.
- 複数のパスワードを管理する必要がある.

そこで, 個人の持つ生体の特徴を利用したバイオメトリクス認証技術を, UNIX システムのログイン認証に利用することを検討する. これにより, パスワードを記憶する必要がなくなり, また他人へのなりすましを防ぐことができる.

本研究では, UNIX システムのログイン認証に, 多くのシステムで用いられている PAM(Pluggable Authentication Module) を利用した.

2 バイオメトリクスを用いた個人認証

バイオメトリクスを用いた個人認証は,

- 普遍性 (誰もが持っている特徴である)
- 唯一性 (本人以外は同じ特徴を持たない)
- 永続性 (時間の経過とともに変化しない)

を備えた生体の特徴を用いて本人を自動的に確認する技術である.

本研究では, NTT データ社の IC カードリーダ一体型指紋認証装置 *SmartBIO* を用いた.

この装置は, 接触型 IC カードリーダと光学式指紋読取装置からなり, USB を用いて PC 本体と接続する.

IC カード内に指紋の特徴点データを保存しておき, 指紋認証装置内部で認証を行なう. このとき指紋の特徴点データが指紋認証装置の外に出ることはなく, 認証が成功したかどうかが暗号化されて外部に通知される.

3 PAM

PAM(Pluggable Authentication Modules)[2] は, OSF-RFC 86.0[1] で提案されたログイン認証や他の様々な認証を 1 箇所にまとめるための枠組である.

従来の UNIX では各プログラムに認証方法が埋め込まれているために, 認証方法を追加・変更しようとする場合には, 各プログラムを変更する必要があったが, PAM を用いることで, モジュールを追加し, PAM の設定ファイルを変更するだけで導入することができる. これは, モジュールに様々な欠陥が発生したときに, すみやかにモジュールを交換できることを意味している.

PAM の実装には以下のようなものがあり, 一般的なモジュールはソースファイルレベルでの互換性がある.

- Solaris PAM (Solaris で採用)
- Linux-PAM (各 Linux, FreeBSD で採用)
- OpenPAM (FreeBSD-Current で採用)

今回は FreeBSD 4.6.2-RELEASE 上の Linux-PAM 0.65 を使用した.

PAM による認証の形態

PAM を用いた認証の手順は図 1 のようになっている.

まず認証を必要とするプログラムが PAM に認証の要求を行う [A]. 要求に応じて, PAM は設定ファイルから設定を読み込む [B]. 設定に従いモジュールに認証の要求を伝える [C]. モジュールは認証を行い, 結果を返す [D]. 設定された条件に合致した結果が得られた場合プログラムに成功を, 得られなかった場合は失敗を, それぞれ返す [E].

Application to UNIX login authentication of biometrics
†FURUKAWA Hideo
‡HANAWA Toshihiro
§Dept. of Information Technology , Tokyo University of Technology

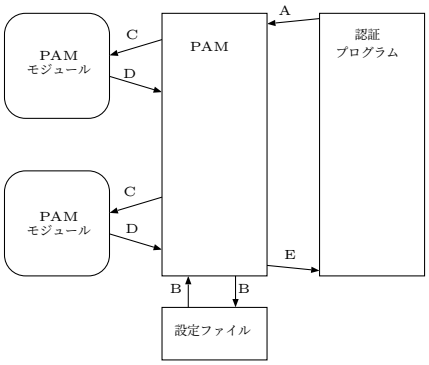

図 1: PAM による認証の形態

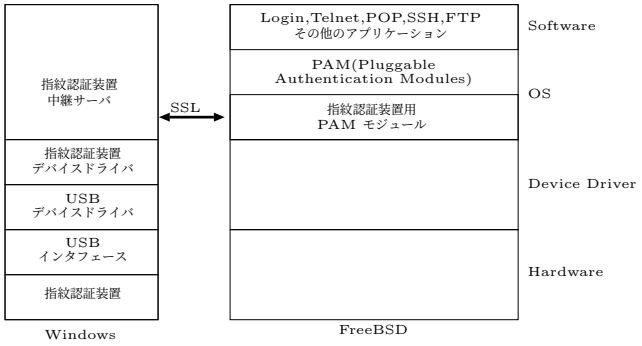

図 2: システム構成

4 実装

SmartBIO で得た認証結果を PC と暗号化通信する必要があるが, UNIX 用デバイスドライバが存在せず, プロトコルも公開されていないため, 直接 UNIX マシンに接続することができない. そこで, 既に提供されている Windows 用のデバイスドライバを利用し, UNIX 側に認証結果を通知することとした.

Windows 側に指紋認証中継サーバを置き, FreeBSD 上の PAM モジュールからネットワーク経由で指紋認証装置を利用できるようにする. その際, 指紋認証中継サーバと PAM モジュール間は, SSL で認証と暗号化をおこなう.

今回のシステムの構成を図 2 に示す.

PAM モジュールは認証要求とユーザ名を受け取り, SSL 経由で Windows 上の中継サーバに送信する. 中継サーバは IC カードを利用して指紋認証を実行. 指紋認証が成功した場合にユーザ名と IC カードのユーザ ID を照合し, 結果を返信する.

SSL は FreeBSD 側に OpenSSL 0.9.6e を, Windows 側に OpenSSL 0.9.5a をそれぞれ使用し, プロトコルは SSLv2, SSLv3, TLSv1 いずれも利用可能である.

5 評価

システムに実際に組み込み, キー入力に慣れている人のユーザ名の入力終了から認証が終了するまでの時間を計測した.

環境は,UNIX 側が CPU: Pentium4 2.4GHz, OS: FreeBSD 4.7-RELEASE, Windows 側が CPU: Pentium3 800MHz, OS: Windows2000 である.

パスワード認証のみの場合, パスワードが簡易な場合平均 1.5 秒で, パスワードが難しい場合平均 3.0 秒で終了した. バイオメトリクス認証のみの場合, 平均 6.7 秒で終了した. なお中継サーバが要求を受け取り, 認証して結果を送信するまでの時間は平均 6.3 秒であった.

6 結論

本研究で, UNIX システムのログイン認証に, パスワード認証に変えて指紋認証を導入した結果, 5 秒程度の認証にかかる時間の増加で, 利用者の負担を軽くし, セキュリティーを高くすることができた.

また, 現在は UNIX のログイン認証のみ可能であり, Telnet や SSH 等の遠隔ログイン時には, 指紋認証を利用することができない. 本研究で実装した中継サーバを応用し, 遠隔ログイン時の認証に指紋認証を利用できるよう, システムを拡張することを検討している.

謝辞

本研究に際し, SmartBIO 及び開発キットをお貸し頂いた, 株式会社 NTT データに深く感謝します.

参考文献

[1] V.Samar, R.Schemers, Unified login with Pluggable Authentication Modules (PAM), http://www.opengroup.org/tech/rfc/rfc86.0.html

[2] Andrew G. Morgan, The Linux-PAM System Administrators' Guide, http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html