3F-5

LDAPを用いたパスワード管理システムの構築

枡上昭広、上原稔、森秀樹
sabo_ami@mo.cs.toyo.ac.jp,{uehara,mori}@cs.toyo.ac.jp
東洋大学工学部情報工学科

1. はじめに

現在、一般に用いられているオペレーティングシステムが備えているセキュリティ機能がパスワードによるユーザ認証システムである。また、それらで使用されるアプリケーションも同様にパスワードによるユーザ認証システムを使用している。これらの認証システムで使用されるパスワードはオペレーティングシステムやアプリケーションごとに異なっているため、使用するリソース、ネットワークが増加するとユーザはそのパスワードの管理を強いられる。そこで本研究では、UnixやWindowsNTなど異なるオペレーティングシステムが存在する複数ネットワーク、ユーザ認証を必要とする複数のアプリケーション使用状況下で、唯一のパスワードを使用したアクセス、また対象リソースに対応したパスワードの参照を可能にするパスワード管理システムを提案する。

2. 関連研究

このような機能を実現する既存のアプリケーションとして、MacOS9に実装されているキーチェーン[1]がある。これは複数のパスワードを一括管理するものである。ローカルにユーザ名、パスワード、リソース名を必要に応じ暗号化して保存し、認証されたユーザのみ自動的に対象リソースを使用できるシステムである。これにより、ユーザは MacOS9にログインする時のパスワードを使用するだけで他のネットワークのリソースを使用できる。しかし、対応するプラットフォームが MacOS9に限られることや、管理者はユーザのキーチェーンに登録したリソースが利用できるなどの機能の問題点を抱えている。本研究では、管理するユーザパスワードに関するネットワーク、アプリケーション、ユーザ情報等をLDAP(Lightweight Directory Access Protocol)[2]サーバ上に保存する。そのため、ユーザはプラットフォームを気にすることなく、リソースのパスワードを参照することができる。

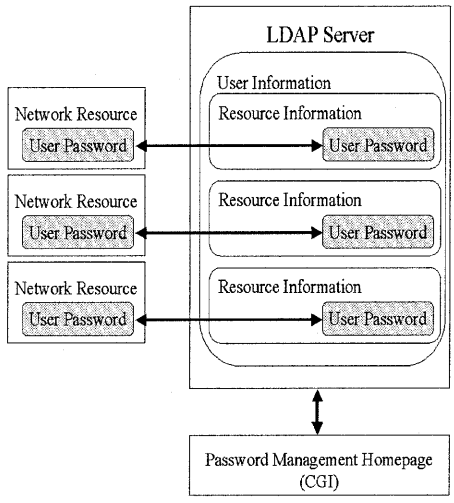

図1 システム概要図

3. 概要

本研究で提案するシステムは、図1で表されるコンポーネントから構成される。本パスワード管理システム対応したオペレーティングシステム、アプリケーションでは、LDAPサーバに保存されたパスワードが各リソースのオリジナルパスワードとなり、LDAP サーバ上のパスワードをパスワード管理ページより変更することにより、各システムのパスワードを変更することができる。対応していないリソースでは、パスワードのコピーとなるので、参照することができる。リソース情報ディレクトリのユーザパスワードは暗号化され、ユーザがパスワード管理ページより参照、変更される個人に関する情報

Password Management System Using LDAP
MASUGAMI Akihiro
Department of Computer and Science
Toyo University

はSSL(Secure Sockets Layer)[3]を使用した接続によりセキュリティを保たれる。

これらによってユーザはひとつのパスワードを記憶するだけで複数の異なるリソースにアクセスすることが可能となる。このパスワードを「メタキー」と呼ぶ。

3.1 データベース構成

LDAPサーバ内には個人のディレクトリが配置され、そのディレクトリにはネットワークリソースのユーザパスワードを含むリソース情報が保存されている。リソース情報ディレクトリのパスワードとネットワークリソースのユーザパスワードはそれぞれ同様のパスワードが保持される。次にリソース情報ディレクトリの詳細を図2に示す。このディレクトリにはネットワークリソースへのアクセスに必要な情報が保持される。NetworkResourceName はネットワーク名が、ResourceApplicationName には対象アプリケーション名が保存される。そして、UserName, UserPassword にはリソースの認証に必要なユーザ名、パスワードが保存される。

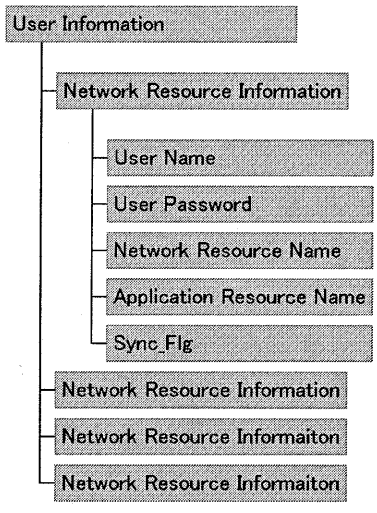

図2 ユーザ情報ディレクトリ

3.2 動作概要

ユーザは対象となるネットワークリソースへアクセスするための情報をパスワード管理ページより、LDAP サーバへ登録する。登録したパスワードはメタキーより参照することができる。ユーザがネットワークリソースへアクセスする時、本システムに対応したリソースでは LDAP サーバ上のユーザパスワードがオリジナルパスワードとなり、ユーザはメタキーのみでアクセスすることができる。対応していないリソースではユーザパスワードのリマインダーとしての役割を果たす。また、ディレクトリ内のSync_Flg[4]は WindowsNT,UNIX ネットワークのユーザログインパスワードを必要に応じ、同期化させる。

4. 今後の課題

今後の課題として、以下のような事項が挙げられる。

- 暗号化されたパスワードの安全性、運用性についての改善
- Windows2000 で提供されている Active Directory[5]への結合とシステムの実装
- リソースのパスワードを LDAP サーバ上への保存を容易にする API の開発

5. おわりに

本論文ではユーザがリソースに認証されるために必要な情報を LDAP サーバ上に配置し、「メタキー」と呼ばれる同一のパスワードを用いて複数のパスワードできるシステムを提案した。

---

[1] Apple computer Corporation
http://www.apple.co.jp/macos/feature4.html

[2] W.Yeong,T.Howes,andS.Kille,
"Lightweight Directory Access Protocol,"
RFC 1777,March 1995

[3] Netscape Communications "SSL 3.0 Specification"
http://home.netscape.com/eng/ssl3/ssl-toc.html

[4] 枡上昭広,上原稔,森秀樹
LDAPを用いたパスワード同期システムの構築
第59回情報処理学会全国大会 1999

[5] Microsoft "Windows2000 技術資料"
http://www.microsoft.com/japan/windows2000/server/technical/directory/