基於安全 LDAP 伺服器之整合服務認證系統設計與實現

李明坤　楊中皇

高雄師範大學資訊教育研究所

摘要

網路世界裡，辨識身分是一個大問題，當越來越多的人開始使用網路服務時，身分認證的問題就接踵而來。網路上提供服務的伺服器眾多，一個人擁有兩個以上的帳號並不稀奇，但要去記得每個帳號與密碼並不是一件容易的事情，而且系統管理員要去管理每一部主機上的帳號也是一件棘手的事。假設有一個可以儲存所有人帳號與密碼的系統，換句話說，使用者只要記住一個帳號，使用網路服務由這個系統認證，一但認證成功，便可登入使用網路資源。如同一個中央管控機制，集中所有資料，負責身分辨識與帳號管理工作，這樣子管理將會變成十分方便。LDAP 是一個標準通信協定，它支援許多認證與安全的選項，將 LDAP 伺服器視為認證伺服器，可以提供非常好的認證與帳號管理功能，加上本身所支援多項的安全功能，保障網路服務存取的安全。

關鍵字：authentication、LDAP、PAM、NSS

1. 前言

複雜的網路環境使各組織需要大量的目錄，用以識別多個作業系統、應用程式、網路服務與企業內部與外部的用戶。隨著組織實施的目錄愈來愈多，要有效的控制、管理與存取資訊變得非常困難，更甚者導致管理成本超支，生產力下降，並且可能造成資料的不一致。網路服務多要求每位使用者有一個使用者帳號和密碼，作為識別使用者身份。很少有一個網路服務允許使用者透過一個通用帳號可以使用多種服務。使用者必須申請個別帳號來存取每一種要求認證的網路服務。當越來越多的人開始使用網路提供服務時，身分認證的問題就浮現出來。網路上提供服務的主機眾多，一個人擁有有兩個以上的帳號並不稀奇，就如同一個人擁有兩張以上信用卡一樣平常。但是要去記得每個帳號與密碼並不是一件容易的事。假設有一個系統可以儲存所有人的帳號與密碼，換句話說，使用者只要記住一個帳號，即可經由這個系統認證去登入使用其他服務，這將會變成十分方便。如同一個中央管控機制，集中所有人資料負責管理工作。

上述的問題，有業者提供相關解決方案， Netscape 是最早推出 LDAP 整合網路服務產品的公司，它的作法是將使用者相關資料，包括帳號、密碼、電子郵件與使用者姓名等資料皆儲存在 LDAP 伺服器裡面，當網頁伺服器或是郵件伺服器需要使用者帳號與密碼認證的時候，就交由 LDAP 伺服器作認證，一但認證成功，就可以取用網頁伺服器或是郵件伺服器上的資源。另外

還有 Novell 的 eDirectory 以及 Microsoft 的 Active Directory。上述產品皆為商業軟體，所提供的功能與服務自有一定水準。使用者不僅要花錢購買，若是要修改部分功能滿足需求，似乎較難以達到，只能被動處於等待產品更新。開放原始碼計畫中的目錄服務工具--OpenLDAP 也可以達到上述部分功能，它可支援多種認證的方式有 certificate-based 認證、Kerberos 認證、明文密碼、摘要認證(digest authentication)、智慧卡(smart card)與 SSL，且具有許多安全功能選項，足以成為安全認證伺服器。因為是開放原始碼，使用者可以免費下載與自由修改部分程式碼，滿足自己對功能上的要求。

傳統的 UNIX 系統使用者密碼用 crypt 函式加密儲存在 /etc/passwd 中，使用密碼對用戶進行認證，使用者輸入的密碼經過 crypt 加密後，再和 passwd 檔中的密碼進行比對。為了讓使用者讀得到，權限必須設定為 0644，等於編碼後的密碼可以被登入的使用者讀到。為避免使用者利用 crack 這種公用程式破解 crypt 加密密碼，Linux 在安裝時多半預設使用 shadow 再加上 MD5 來編碼，passwd 檔中的密碼被轉到 /etc/shadow 下，檔案的權限只有 root 才能讀到。MD5 是一種較先進的編碼方式，255Bytes 的編碼長度可以大量延長被破解的時間。如此作法卻面臨兩個問題，第一，管理員自由設定系統的安全，系統可能設定是 MD5 加上 shadow，或是 MD5 但不加 shadow，甚至用其它的認證方式(像 kerberos)，但是像 login 這種登入程式如何判斷系統採用何種認證方式；第二，網路服務愈來愈盛行，許多服務被開發出來，這些服務要採用何種方式進行系統認證。

上述問題的方法可以使用 PAM 進行統一身份的認證。PAM，嚴格一點稱為Linux-PAM (Pluggable Authentication Modules for Linux) 使用在Linux上可插拔式認證模組，是一組能讓系統管理員自由切換，選擇認證模組來驗證使用者的共享函式庫。利用PAM模組統一各伺服器間認證的問題。

2. 文獻探討

2.1 LDAP

LDAP (Lightweight Directory Access Protocol) 由密西根大學所發明定義於 RFC 1777，是一種衍生至 X.500 且運作在 TCP/IP 架構上的目錄服務存取協定，目前最新版本是第三版。LDAP 如同資料庫般可以儲存資料，但多是描述性或屬性為主資料。這些資料用途多是提供被讀取，較少經常變動。資料以樹狀結構組成，允許資料按階層分散在不同區域，因此無論從任何一部 LDAP 伺服器所詢問到的資料都會相同。樹狀結構上的每一個物件由多種屬性與數值組成，物件可以代表示是一個使用者、一部電腦，甚至一個部門，每個皆有一個識別名稱(DN)，定義於 RFC 1779，識別名稱(DN)命名是由上層父節點的 RDN 串結而成，且是唯一的。

LDAP 伺服器裡頭的資料是以 LDIF(LDAP Data Interchange Format)格式來儲存，它是一種純文字方式來呈現資料的格式。這種格式是依行(line)來作區隔，冒號之後接的是資料的屬性，例如：

dn: cn=david,ou=People,dc=example,dc=com

uid: david

cn: david wang

objectClass: account

objectClass: posixAccount

objectClass: top

....

這種格式容易在LDAP伺服器之間轉送、備份與做大量資料的修改。

2.2 PAM 模組

PAM (Pluggable Authentication Modules)使用在Linux上可插拔式認證模組，是一組能讓系統管理員自由置換，選擇認證模組來驗證使用者的共享函式庫。安裝這些模組，勿需重新編譯應用程式就可以安裝使用。其最大的優點是它的彈性和可擴充性，PAM能夠提供的認證方式多種多樣，從絕對信任(pam_permit)到智慧卡(Smart Card)。可以隨意切換認證機制，按實際需要來制訂認證模組。

PAM可以視為是「要求認證服務的應用程式」與「提供認證服務的認證機制」之間的溝通介面。從整個認證系統來看，PAM是認證系統的應用程式介面(API)，或者說是前端；而認證機制模組則是後端，如圖1。

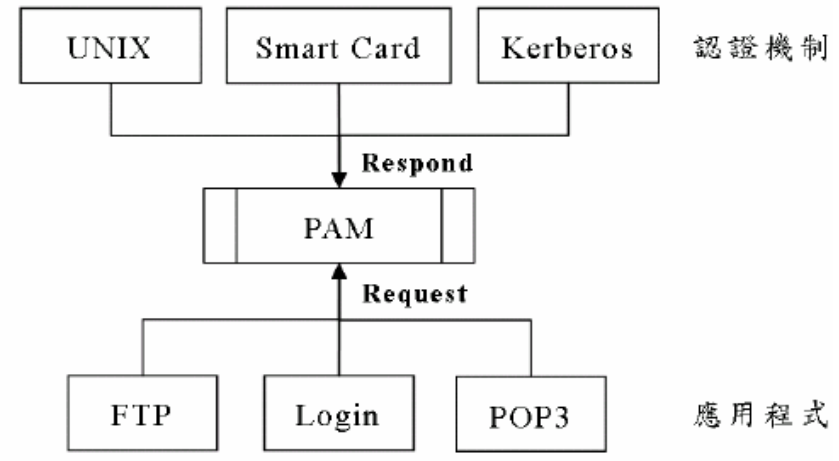

圖 1. 顯示 PAM 和認證機制與應用程式之間的關係

舉例來說，從FTP下載檔案，必須先輸入使用者名稱和密碼才能登入取得服務，就FTP而言，判斷使用者的帳號密碼是否有效與它無關，FTP只是將這組認證資訊傳給PAM，PAM會根據 /etc/pam.conf 的設定值來決定如何認證，接下來相關認證的過程，例如比對使用者名稱和密碼，就交給後端的認證機制模組來做。最後，PAM 將認證結果成功或失敗傳回值給FTP引擎，完成整個認證過程。

PAM共有四種認證型態(type)，分別是auth(認證)，account(帳號管理)，session (對話管理)，和password (密碼管理)，代表了不同種類的認證程序，也稱為PAM模組介面(PAM module interfaces)。PAM設定檔以空白或是[Tab]分欄，分為四個欄位，由左至右分別是：認證型態(module interface)，控制旗標(control flag)，模組路徑(module path)和模組引數(module arguments)當前端程式呼叫PAM 的時候，PAM 除了依據設定檔作不同型態的認證外，還必須依照控制旗標的設定來傳回認證成功(PAM_SUCCESS)或是認證失敗(PAM_FAILURE)。

預設的控制旗標有四個：required，requisite，sufficient，optional。

由於PAM是開放標準，目前Linux上絕大部分伺服器皆透過PAM機制做登入認證，相關的模組數量很多，各種網路服務自行開發自己的認證模組，表一所列為部份PAM基本模組。

表一： PAM 基本模組

模組名稱	適用型態	說明	相關檔案
pam_access	ac	限制使用者，群組或網路位址	/etc/security/access.conf
pam_cracklib	pw	限制密碼內容如長度，大小寫…	
pam_deny	all	禁止存取，固定傳回值：失敗	
pam_ftp	au	控制匿名 ftp 的使用	
pam_group	au	賦與使用者群組資格	/etc/security/group.conf
pam_krb4	au ac pw	kerberos 驗證及 ticket	
pam_limits	se	限制系統資源的使用	/etc/security/limits.conf
pam_nologin	au	禁止除 root 以外的使用者登入	/etc/nologin
pam_permit	all	允許使用者登入	
pam_rootok	au	允許 root 不使用密碼	
pam_time	ac	服務時間限制	/etc/security/time.conf
pam_unix	all	標準 UNIX 認證模組	

在 PAM 中，使用者密碼一般是由模組 unix 來認證，更改/設定則是由 cracklib 控制，另外，limits 可以用來限制資源的使用，time 則可以用登入

時間來限制。PAM 可以根據不同的需要引用不同的 PAM 模組，形成模組堆疊(Stacked Modules)，彈性地達成系統管理員的複雜要求。

2.3 NSS 模組

NSS(Name Service Switch，名稱服務切換)模組可讓管理者指定欲詢問的檔案或目錄次序，以取得所需的資訊。利用 LDAP 伺服器作為使用者認證的作法，是將要驗證的帳號資料置於同一目錄下，然後再導向此目錄。利用 NSS 模組充當名稱解析轉向器，設定名稱查詢首先詢問 LDAP 伺服器。例如欲查詢某主機資訊可以去本機的/etc/hosts 詢問，或轉向 DNS 查詢，或是本研究中的利用 LDAP 伺服器查詢，解析資訊來自源。若要使系統先詢問 LDAP 目錄，設定先從 LDAP 伺服器目錄查詢密碼檔案、遮蔽檔案以及群組檔案設定如下。

passwd: ldap files

shadow: ldap files

group: ldap files

這個設定檔表示先從 LDAP 伺服器開始查詢，查無資料之後才換到 files(也就是本機的/etc/hosts)。

3. 系統架構

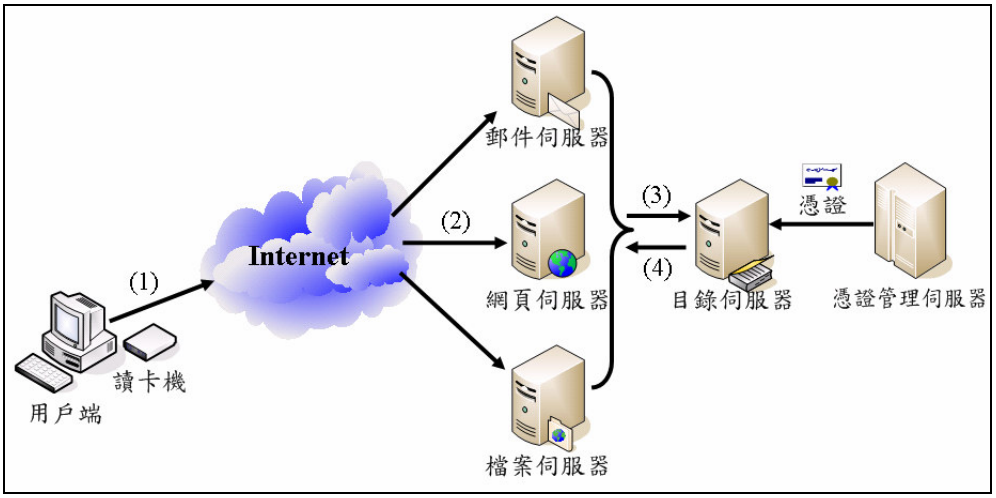

圖 2. 認證系統架構

本研究系統架構如圖 2 所示，主要運作模式是主從式架構，分成兩個部份，一部分是伺服端，接受服務請求，以 LDAP 伺服器當認證伺服器，CA 是憑證管理伺服器，憑證管理中心可將申請通過的憑證傳送到 LDAP 伺服器，共使用者隨時下載；另一邊是用戶端，使用者輸入帳號與密碼，或是利用所隸屬的讀卡機插入智慧卡來讀取儲存在卡片內的使用者資訊。使用者向應用程式提出服務要求，經由置入 NSS 模組轉向 LDAP 查詢使用者資訊，並

利用所設定 PAM 模組驗證資料的有效性，PAM 依據設定檔作不同型態的認證，分別呼叫所使用的共享函式進行驗證工作，一但驗證成功，傳回值認證成功(PAM_SUCCESS)，否則傳回值驗證失敗(PAM_FAILURE)。一但認證成功，應用程式將會通知使用者可以成功登入使用網路資源。整個認證系統流程圖如圖 3 所示。

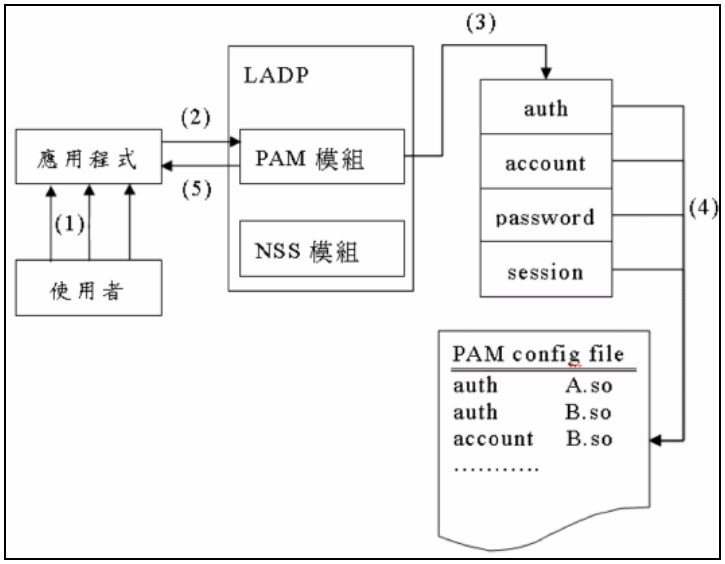

圖 3. 認證流程圖

4. 整合服務認證系統實作

4.1 系統實作

在系統服務上，許多公司用 LDAP 作為公司"白頁"解決方案，因為許多 email 與行事曆應用都與 LDAP 相容。Netscape、Mozilla、Evolution、Outlook、KMail 與許多 email 用戶端程式都強力支援 LDAP，例如 Outlook 查詢 LDAP 伺服器目錄或新增使用者帳號(見圖 4)。

圖 4. 利用 outlook 查詢 LDAP 伺服器帳號

LDAP 的圖形化編輯器及瀏覽器，例如：GQ、Java LDAP Borwser/Editor 與 Softerra LDAP Administrator/Browser 用來管理帳號作業，但是多僅能查詢或管理目錄資訊，缺乏整合各項服務功能。Miscrosoft 的 Active Directory 與 Novell 的 eDirectory 聲稱具有全目錄服務的功能，可整合各項網路服務。Active Directory/ Miscrosoft 以網域(domain)的概念，將網域內的電腦與使用者視為管理物件，預設利用 Kerberos 為認證協定來去認證登入網域的任何物件，物件一但認證成功，既可依所設定權限存取網域內的資源。上述產品為商業軟體，使用者需花錢購買，無法修改部分功能滿足需求，只能被動處於等待產品更新。本研究利用 Borland C++ Build 設計一個簡易的圖形化整合認證登入系統(見圖 5)，透過本程式除了可以連接 LDAP 伺服器查詢使用者資訊，也可以提供登入各種網路服務伺服器的單一認證窗口。

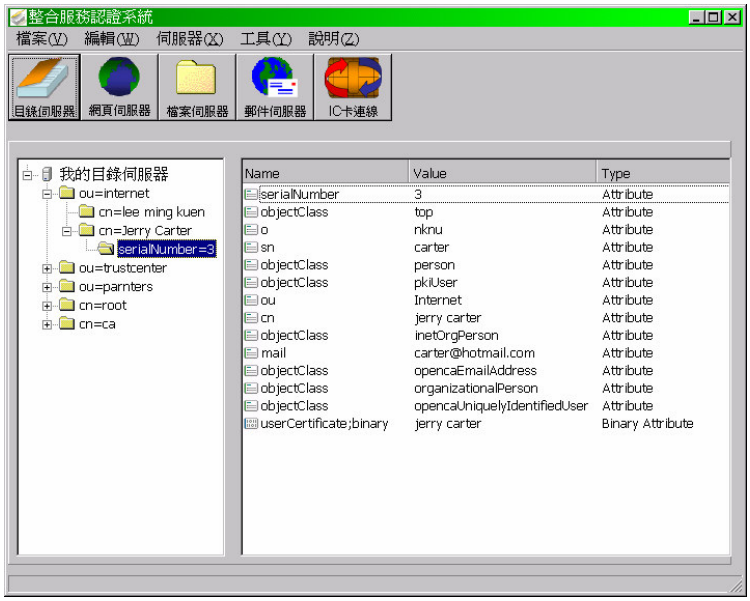

圖 5. 整合服務認證系統

登入步驟可以使用輸入使用者帳號與通行碼，透過認證手續(見圖 6)提出服務要求。因為 LDAP 物件階層式的命名方式可確保使用者名稱具獨立性，就算是相同的帳號名稱，但因所屬的父節點 RDN 不同，可以擔保該節點 DN 是本目錄樹唯一識別名稱，經由儲存物件的 LDAP 伺服器來認證登入使用名稱是否有效。也可以使用儲存有核發的公開金鑰憑證、私密金鑰與相關使用者資訊的智慧卡，只要使用隸屬的讀卡機就可讀出資料，進行驗證工作。因為智慧卡難以複製的安全特性，對使用者密碼又多一層保護。

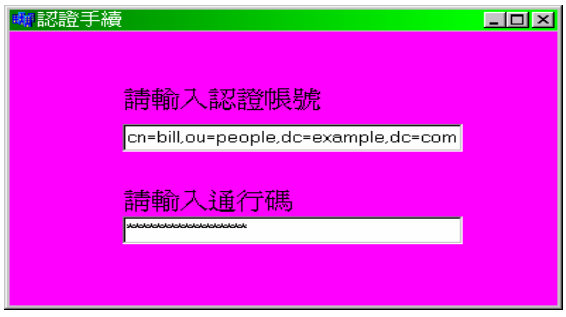

圖 6. 認證手續

為簡化登入不同主機須重新輸入帳號的麻煩，LDAP 可支援指定一群使用者存取特定主機服務，達到使用單一身分可以存取多重服務的目的，省卻記憶多組帳號麻煩，也可做到單一簽入(Single sign on)優點。實作方式就是在 LDAP 建立一筆 ldif 資料，例如：

dn: uid=bill,ou=people,dc=example,dc=com

uid: bill

cn: bill wang

objectClass: account

objectClass: posixAccount

objectClass: shadowAccount

loginShell: /bin/bash

uidNumber: 680

gidNumber: 200

homeDirectory: /home/bill

userPassword: {crypt}HoYmlMd5giAE

host: ldap.example.com

host: ftp.example.com

host: www.example.com

這筆資料建立在 LDAP 伺服器裡面，使用者就可用 bill 帳號登入到 ldap、ftp 和 www 主機存取資源。

以 LDAP 伺服器做為認證伺服器，只要將應用服務伺服器認證機制更換為 PAM 機制的認證模組，即可將認證工作交由 LDAP 伺服器來擔任。目前 Linux 系統裡，Telnet、POP3、IMAP、FTP、WU-FTP 與 Apache 等伺服器的認證皆可透過 PAM 機制作認證工作。Apache 可借目錄之便，設定公司內部人員存取檔案權限。另外，代理伺服器 Squid 也支援，用來限制僅內部人員才有權使用網路資源。

4.2 安全問題

現在將所有資料集中在同一目錄，裡面存放許多敏感的資料，安全問題的顧慮就非常重要。有些資料要避免非授權用戶讀取，雖然所有資料經過雜湊函數運算成雜湊值，但也可能被用字典攻擊法破解，更甚者，任何人都可能擷取用戶端與伺服器間的連線，偽造訊息或是重送(replay)餵給另一端使用者，或是使用用戶端的權限去更改伺服器資料。OpenLDAP 有多種安全措施可以避免這些事情發生。

存取控制清單(ACL，Access Control List)限制誰可以讀取與誰可以修改的權利，有效分配每個使用者存取服務的權限，讓不相關的人員沒有機會接觸敏感的資料，防止未被授權人士入侵。LDAP 提供一套存取控制的語法來保護不同資料的存取，這對儲存密碼在 LDAP 目錄裡面來說非常重要，它的語法格式如下：

access to attr=userpassword

by self write

by anonymous auth

by * none

這表示允許使用者可以變更自己密碼，限制 userpassword 只能用於認證，未授權使用者不能更改其他人的密碼。這與讀取權限不同，使用者永遠都無法獲得 userpassword 屬性的值，伺服器只會比對使用者輸入的密碼與存放在目錄的值，意思是說密碼從未送出伺服器，不用擔心被第三者擷取。

LDAP 提供兩種可用來保護密碼的機制，一個是以 SASL 來支援較安全的認證，SASL(Simple Authentication and Security Layer)定義在 RFC2222 可以提供認證與授權功能的 API 與模組，模組化的 SASL 可支援許多的認證機制，如 Kerberos IV/V 到 CRAM 與 DIGEST MD5。另一個是支援使用 TLS/SSL 的加密與認證方式。TLS/SSL 使用 X.509 憑證方式提供證明伺服器真偽以及保護密碼在網路上傳輸。同樣地，對伺服器而言，它也可以證明使用者真偽。憑證的取得可以向知名廠商購得，例如 Entrust，Versign 廠商。或是便宜作法可以自行架設 CA 發行憑證，利用 OpenSSL 工具程式，自己產生 CA 的秘鑰與 CA 的憑證，自行簽署，例如：

% openssl genrsa –des3 –out ca.key 2048

% openssl req –new –x509 –days 365 –key ca.key –out ca.cert

然後再產生 LDAP 的私鑰與憑證，LDAP 伺服器憑證由自行產生的 CA 秘鑰簽署。如此，當 LDAP 伺服器啟動時，就可以使用 TLS/SSL 功能，也就是下次登入時的通信協定改成 ldaps:///URL，在會談過程當中提供傳輸層階段的加密，可提供密碼的保護。

5. 結論

LDAP 伺服器當作認證伺服器，安全性遠勝於簡單的密碼驗證，並且有極大的擴充空間。本研究利用 LDAP 伺服器提供的帳號管理與可置入 Linux 系統伺服器的 PAM 認證模組，設計一個整合服務認證程式，提供目錄管理與服務整合的功能，減少公司軟體成本支出與簡便帳號管理工作。未來 LDAP 的應用將會更加廣泛，期待整合網路服務，便利資源的分享。

6. 參考文獻

1. Andrew Findlay(2002), Security with LDAP, http://www.skills-1st.co.uk/papers/security-with-ldap-jan-2002/security-with-ldap.singlesided.pdf

2. Brad Marshell, System Authentication using LDAP, http://quark.humbug.org.au/publications/ldap/system_auth/sage-au/system_auth.html

3. G.Carter(2003), LDAP System Administration, O'Reilly

4. M.Smith and T.Howes(1997), LDAP: Programming Directory-Enabled Apps, sams

5. M. Wahl et al.(2000), "Authentication Methods for LDAP", IETF RFC 2829, http://www.ietf.org/rfc/rfc2829.txt

6. Novell eDirectory, http://www.novell.com/

7. OpenLDAP, http://www.openldap.org/

8. PADL's nss_ldap, http://www.padl.com/OSS/nss_ldap.html

9. PADL's pam_ldap, http://www.padl.com/OSS/pam_ldap.html

10. T.Jackiewicz(2004), Deploying OpenLDAP, APress

11. W.Stallings(2003), Cryptography and Network Security: Principles and Practices, e3, Person Education