The Integration of Network Service Authentication Design and Implementation for Secondary and Elementary School

Chih-ming Hung
National Kaohsiung Normal University
imeuimeu@yahoo.com.tw

Chung-Huang Yang
National Kaohsiung Normal University
chyang@nknucc.nknu.edu.tw

摘要

本研究以台灣目前國中小學的網路環境及需求為背景，探討校園中認證整合的問題。在基礎架構方面，我們以 OpenLDAP 整合校園中常用服務的認證機制：FTP、Samba、Open Webmail 帳號；在管理實務上，我們發展管理者介面：AIM(Authentication Integration Manager)及一般使用者介面：SHS(Self-help Service)，藉此來同步 OpenLDAP 及 SFS(School Free Software)學務系統、Moodle 課程管理系統之間的認證資訊；除此之外，我們也經由中文化來導入 LAM(LDAP Account Manager)，使得認證整合、密碼同步及帳號管理問題得以一併解決，將有助於增進校園資訊化的腳步及強化校園的資訊安全。

關鍵詞：認證整合、密碼原則、目錄服務、LDAP。

Abstract

This research is based on the present network environment and demand for Secondary and Elementary school in Taiwan; it will discuss the authentication and integration in the campus. For basic frameworks, we used OpenLDAP to integrate the common used service authentication system: FTP, Samba, Open Webmail Account; as for the practical administration works, we developed administrator interface: AIM(Authentication Integration Manager), and common user interface：SHS (Self-help Service), by using this to synchronize the authenticated information of Openldap, SFS(School Free Software) Student Affair System and Moodle Course Management System. Apart from this, we also translated it into Traditional Chinese to lead in LAM(LDAP Account Manager), establish integrated authentication and password synchronization as well as resolved the problems of account management. This will help us to build up the steps for campus information technology and reinforce the campus information security.

Keywords: Authentication integration, Password Policy, Directory Service, LDAP.

1. Introduction

Since 1999, the government stimulated the domestic demand policy; LAN has become a part of basic infrastructure in Secondary and Elementary school. It followed with constructing all types of network service. On the basis of the safety reason, each type of service will have the authentication mechanism. It means that at the same time the increasing services will bring on the same ratio growth of the complication for authentication management.

More seriously, the authentication are not only the problems of the management but also the problems of the information security which was come from distractive authentication mechanism and which have been highly focused on. As the issues of information security has been valued recently, authenticate integrations such as LDAP and Kerberos etc. are also being actively discussed. Therefore this article is to explore the current issues of the process leading in integrated authentication in the Secondary and Elementary School

1.1 Research Motivation

ID/PW is the only passage used in the service. Therefore, the authentication was poorly designed will cause failure of the service, this will seriously influence the business work. However, information technology was not related to competition in the Secondary and Elementary School, relatively the authenticate system is lack of careful design.

We often see id/pw being over distributed, which means that each type of service network uses different authentication information, meanwhile, users often being forced to accept such poor quality authentication system. Another extreme type is : sharing the same id/pw. It is undeniable that these situation are often existed peacefully in the Secondary and Elementary schools, that is because the authentication integration has not yet being taken seriously. Take Kaohsiung City for example, the information center of Education Department held over hundreds of sessions for the network administrators[6] but none of it was about the authentication integration topic. We may foresee that this type of problem will be one of the main troubles for impetus information technology. Therefore, we believe that it’s in urgent to integrate the network authentication in the Secondary and Elementary School.

1.2 Research Aims

To induct the authentication system successfully, there are some tools needed to achieve following goals:

(1) Practical basic framework: This article will explain the practical works on OpenLDAP integrated FTP, Open Webmail and Samba authentication systems and introduce the web-based AP, SFS and Moodel, in common at school.

(2) Develop SHS: Providing web interface for users to change and reset their passwords, may change password on FTP, Open Webmail, Samba, SFS and Moodle simultaneously or individually, as well as support dictionary check, various password policy and hash algorithm.

(3) Develop AIM system: Providing web interface for the administrator setting up the preferences of SHS, password policy group, also changing any user password and synchronizes information between OpenLDAP and MySQL.

(4) Translate LAN into Chinese: The LAM manages especially for each type of account in the LDAP, this will be a extremely convenient tool for processing lead in authentication integration and future information maintenance.

1.3 Research Restriction

The Secondary and Elementary Schools are the continuously headquarter of using Open Source software, due to the limitation of funds. In the article the software used are belong to OSS too, the software version are followed such as FC3 (Fedora Core 3), openldap-2.2.29-1, vsftpd-2.0.1-5, Samba-3.0.10-1, Open Webmail-2.51, Apache-2.0.53-3.3, php-4.3.9-3, LAM1.0, SFS3, Moodle1.5.4.

2. Background Knowledge

2.1 OpenLDAP Integrates FTP Authentication

Linux uses PAM (Pluggable Authentication Modules) /NSS (Name Service Switch) system to control user authentication procedure. The location for configuration files of PAM is beneath /etc/pam.d/ and the configuration file of NSS is located at /etc/nsswitch.conf. Another setting is the global configuratoin file of LDAP client: /etc/ldap.conf, the contents are appointing address of LDAP Server and the Base DN when querying LDAP server.

We suggest that using the tool called authconfig for the FC system, because it can finish all the configurations we mentioned above.

Then, we must set up the file /etc/openldap/slapd.conf on the openLDAP Server side, including the ACL(Access control list) and the database section that can keep account information.

Then, we must create container that stores accounts and groups, for example:

“ou=users, dc=my-domain, dc=edu, dc=tw “and “ ou=groups, dc=my-domain, dc=edu, dc=tw “.

If we need to transfer the existing system accounts, then may use the tools in /usr/share/openldap/migration/ that can output corresponding ldif files that can be exported to LDAP server.

It is essential to get more understanding, because the complication for OpenLDAP related configurations, especially when it involves security issues。

2.2 OpenLDAP Integrates Open Webmail Authentication

To integrate authentication work for Open Webmail[17] can also use the PAM/NSS system.

After installing Open Webmail correctly, also need to install perl-Auth-pam. Meanwhile we need to make sure all prior operation work correctly, and then we can change following settings:

(1) Edit openwebmail/etc/openwebamil.conf: change auth_module attribute value from “auth_unix.pl” into “auth_pam.pl”.

(2) Edit the file openwebmail/etc/ default.conf/auth_pm.conf : change servicename attribute value into “openwebmail”.

(3) Create /etc/pam.d/openwebmail file, this file name is taken from last step’s servicename attribute value, the contents are:

```
auth sufficient /lib/security/pam_ldap.so
auth required /lib/security/pam_unix_auth.so use_first_pass
account sufficient /lib/security/pam_ldap.so
account required /lib/security/pam_unix_acct.so
```

After the settings from above, Open Webmail is able to operate authentication on OpenLDAP via PAM.

2.3 OpenLDAP integrates Samba Authentication

Samba Server is currently the only way to substitute Windows Domain construction, therefore, to integrate Samba authentication is extremely important in the Secondary and Elementary Schools, which are lack of fund very much.

On Samba Server, within the configuration file /etc/samba/smb.conf there are some parameter related to LDAP, these values must be set up according to the practical working environment:

```
passdb backend = ldapsam
ldap server = localhost
ldap port = 389
ldap admin dn = cn=root,dc=my-domain,dc=edu,dc=tw
ldap suffix = dc=my-domain,dc=edu, dc=tw
ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap machine suffix = ou=Machines
ldap ssl = on/off/start_tls
```

In which ldap admin dn's value is the DN used when binding LDAP by Samba, it's corresponding password must be set by using "smbpassed –w" instruction in advance.

Then, we must copy /usr/share/doc/samba-x.x.x/LDAP/samba.schema to /etc/openldap/schema/. Also including this file in the global section at the slapd.conf.

Then, creating essential index in the bdb section:

```
index sambaSID, sambaPrimaryGroupSID, sambaDomainName eq
```

As well as its extra setting for ACL:

```
access to attrs=sambaLMPassword, sambaNTPassword by * auth
```

Then stop slapd and reconstruct index:

```
root#/etc/rc.d/init.d/ldap stop; slapindex - v
```

Finally, we should add Samba account into LDAP, generally, sambaAccount and posixAccount will integrate in the same uid.

Besides, while Samba plays the role of domain controller, integrated Samba account will be more complicated [9] [11].

As shifting UNIX system account to OpenLDAP can use tools like migratation, the miscellaneous matters mentioned above can also use smbldap-tools [10] to assist for completion.

2.4 Moodle: A Course Management System

Moodle is a course management system - a free, Open Source software package designed using sound pedagogical principles, to help educators create effective online learning communities[16].

There are over 100,000 registered users using Moodle all over the world, and currently supports over 70 different kinds of languages, therefore, you can see the popularity of it.

In the authentication administration, Moodle is one of the minorities that supports LDAP authenticated Web-based AP. However, in this article we still integrate by its default method, in which id/pw saved in the "moodle" database in MySQL, there are "username" and "password" these two fields in the "mdl_user" table, using MD5 algorithm to hash the password.

2.5 SFS: Student Affairs System

SFS which was developed by Taiwan Taichung County WaiPu Elementary School, at present there are over eighty modules, and it has won the outstanding award of free software in 2003. At the moment there are over five hundred Secondary and Elementary School in Taoyuan County, Miaoli County, Taichung County and Changhua County are using this system. [3]

SFS3 is used in this research, the staffs' id/pw are preset in the 'sfs3' database, in the 'teacher_base' table the two fields 'teacher_id' and 'login_pass'.

3. Design and Practical Work

3.1 Overall Construction

It contains the application programs for integrated construction, AIM, Self-help Service and LAM system mentioned and explained in the previous chapter, the completed authenticate integration graph is showed at below:

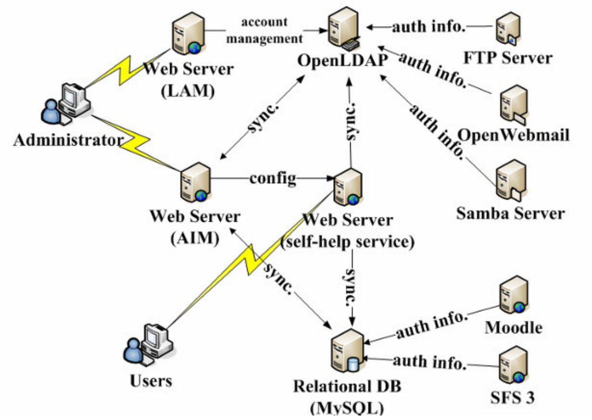


Figure 1: The Integrated Authentication Construction

(1) The administrator creates new accounts and manages accounts through LAM.

(2) The administrator sets up SHS parameters and password policy.

(3) Users input new password in the browser and transmit to the Web Server where SHS is located.

(4) After authentication, SHS inspects new password according to password policy.

(5) After password policy inspection, hash the new password into different type of ciphertext.

(6) Save ciphertext at the RDB and

OpenLDAP, achieves synchronized effects.

(7) Client request authentication information from OpenLDAP for FTP Server, Open Webmail, and Samba Server.

(8) Client request authentication information from RDB for Web-based AP (SFS, Moodle)

(9) All cleartext transmissions take SSL/TLS for security protocol.

3.2 SHS: Change Password and Reset Password

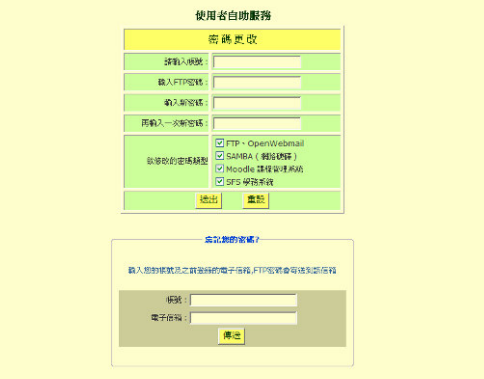
Self-help Service includes two main functions; one is changing password and another is resetting password.

The changing password function is able to alter Linux (FTP and Open Webmail), Samba and Web-Based AP's passwords simultaneously and individually.

The password reset function will send a random password that contains character set of 12 characters to the email address that user registered before.

This system supports 17 types of password policy, 480000 words dictionary file, shadow account function and Windows' highest 24 history password limits.

Figure 2 is the operating diagrams.



使用者自助服務

密碼更改

請輸入帳號：

輸入FTP密碼：

輸入新密碼：

再輸入一次新密碼：

欲修改的密碼類型 ☑ FTP、OpenWebmail ☑ SAMBA（網路磁碟） ☑ Moodle 課程管理系統 ☑ SFS 學務系統

忘記您的密碼?

輸入您的帳號及之前登錄的電子信箱,FTP密碼會寄送到該信箱

帳號：

電子信箱：

Figure 2: SHS Main page

3.3 AIM: Authenticate Integration Manager Interface

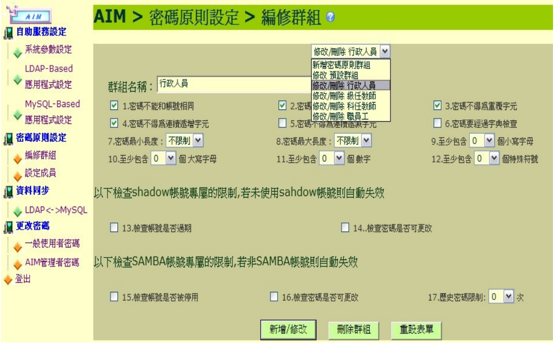
SHS is corresponsive to the general user interface, on the other hand, AIM is located as the administration interface, to provide the administrators to setup the whole system, and then, SHS will take its setup value to operate. The AIM functions are explained as below, Figure 3 and Figure 4 are the operation pictures.

(1) SHS Settings: Setting parameters for SHS system and edit the application program name of SHS interface.

(2) Password Policy Setting: May group the Password policy, apply different password policy according to different user.

(3) Data Synchronization: May synchronize data between OpenLDAP and MySQL, this will be able to apply in the new host initialization.

(4) Batch Changing Password: May provide the administrator to change all users' password and also reset the password.



AIM > 密碼原則設定 > 編修群組

修改/刪除 行政人員
新增密碼原則群組
修改 預設群組
修改/刪除 行政人員
修改/刪除 級任教師
修改/刪除 科任教師
修改/刪除 職員工

群組名稱：行政人員

☑ 1.密碼不能和帳號相同 ☑ 2.密碼 ☑ 3.密碼不得為重覆字元

☑ 4.密碼不得為連續遞增字元 □ 5.密碼不得為連續遞減字元 □ 6.密碼要經過字典檢查

7.密碼最小長度：不限制 8.密碼最大長度：不限制 9.至少包含 0 個小寫字母

10.至少包含 0 個大寫字母 11.至少包含 0 個數字 12.至少包含 0 個特殊符號

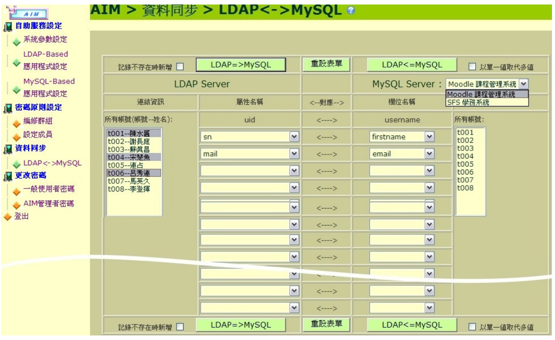
以下檢查shadow帳號專屬的限制,若未使用sahdow帳號則自動失效

□ 13.檢查帳號是否過期 □ 14..檢查密碼是否可更改

以下檢查SAMBA帳號專屬的限制,若非SAMBA帳號則自動失效

□ 15.檢查帳號是否被停用 □ 16.檢查密碼是否可更改 17.歷史密碼限制: 0 次

Figure 3: AIM: Executing Page of Creating a Password Policy Group



AIM > 資料同步 > LDAP<->MySQL

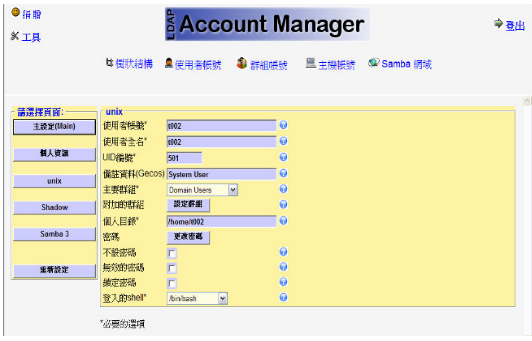
記錄不存在時新增 □	LDAP=>MySQL	重設表單	LDAP<=MySQL	□ 以單一值取代多值
LDAP Server			MySQL Server：Moodle 課程管理系統 Moodle 課程管理系統 SFS 學務系統	
連結資訊	屬性名稱	<--對應-->	欄位名稱	
所有帳號(帳號--姓名): t001--陳水匾 t002--謝長庭 t003--蘇貞昌 t004--宋楚魚 t005--連占 t006--呂秀連 t007--馬英久 t008--李登揮	uid	<---->	username	所有帳號: t001 t002 t003 t004 t005 t006 t007 t008
	sn	<---->	firstname	
	mail	<---->	email	
		<---->		
		<---->		
		<---->		
		<---->		
		<---->		
		<---->		
		<---->		
		<---->		
記錄不存在時新增 □	LDAP=>MySQL	重設表單	LDAP<=MySQL	□ 以單一值取代多值

Figure 4: AIM: Executing Page of Synchronizing Data between OpenLDAP and MySQL

3.4 LAM: LDAP Account Manager

To get the free LDAP administrating program from www is quite easily, for example, PLA (phpLDAPadmin)[18] is one of the most recommended. The appearance of this type of program is to reflect directly LDAP logical construction by the form of tree diagram, to type in DN/PW when log in, not ID/PW. You often see its interface words such as schema and ldif, and these words belong to the special terms for LDAP. As for the beginners of LDAP, it is not the ideal way to present the special terms in tree diagram. Therefore, in the beginning process of integration, we only see this type of tree diagram program as a supportive function, and use more intuitional account administration system – LAM [12].

LAM is not present by the tree diagram, the whole interface almost doesn't use the special terms of LDAP, but matches general account administration habits, to administrate Linux system account and Samba account at the same time. Unfortunately, LAM does not have Chinese interface. Therefore, there are not many local users who can accept it. Therefore we joint the work translating the program into Chinese language; it has been accepted by the LAM developing team [13].



unix

使用者帳號* t002
使用者全名* t002
UID編號* 501
備註資料(Gecos) System User
主要群組* Domain Users
附加的群組
個人目錄* /home/t002
密碼
不設密碼 □
無效的密碼 □
鎖定密碼 □
登入的shell* /bin/bash

*必要的選項

Figure 5: LAM: Setting Linux Account page

At present (2006/06) LAM supports 11 languages, which also includes Traditional Chinese. This system has many praiseworthily functions and design. For instance, it attached with some tools, including uploadable CSV file to add mass accounts; as well as convert the account data into PDF file; also allow user to establish configuration file samples in the complicated environment.

LAM originally contains intuitional operate interface, in addition to support from Traditional Chinese, even if you don't have much knowledge of LDAP, you still can also easily maintain account data in OpenLDAP server through LAM.

4. Discussion and Future Research

Transmitting change of password is the most privacy information, therefore, the security is the most important in consideration. The system we developed will achieve the following goals:

(1) Integration: Take OpenLDAP and MySQL for authentication data storage, being able to alter Linux (FTP and Open Webmail), Samba and Web-Based AP's password simultaneously and individually.

(2) Independent: Unattached in neither the operating system nor other application program.

(3) Security: May transfer cleartext into ciphertext using nine kinds of algorithm: crypt, md5, smd5, sha, ssha, ssh256, Windows LM, Windows NTLM and Windows history password. Also may apply various password policy and dictionary check as well as support SSL/TLS.

(4) Flexibility: The managers can aim at different users to set up each parameter and security principle through AIM system.

(5) Use friendly: By simplicity of webpage interface, let the operation that we mentioned before more transparent and reduce the resistance of the new measure for the user.

In the previous paragraph mentioned, we used OpenLDAP to integrate the authentication service commonly used in the campus, as well as developed some related tools. At the moment there are some research about web-based of SSO(Single Sign-on) based on LDAP,[4] we will work towards this direction as well in the future.

After we changed to LDAP authentication, the changing password system build in the Open Webmail will become invalid, the problem can be solved by adding 'password' module in the /etc/pam.d/openwebmail. The build in changing password system can exist simultaneously with this system. However, our system supports a more complicated password policy.

The system developed in this article was developed from the environment of PHP, MySQL and OpenLDAP. We look forward to support other LDAP server and RDB in the future.

The support of LDAP to password policy is at the draft stage of IETF[8], this indicates that there is a research team which is working on it at the moment. On the other hand, Moodle which was mentioned before in the article, itself contains LDAP authentication module, and there will be more and more database AP support LDAP authentication in the future, until then the integration work will be simplified and completed.

5. Conclusion

This research is focused on the necessity and the inevitability of the Secondary and Elementary School authentication integration, discussing the practical progress and developed essential tools. By AIM, the administrator may establish integrate system; by SHS, may synchronize many kinds of passwords and realize password policy on organization level; and as for the translating Chinese language in LAM administrating system, can assist local LDAP administrator to manage the account data more easily, therefore, this research will have some contribution for carrying out boosting campus information technology and data security, and is valuable for the IT people who are willing to apply authentication integration system.

References

[1].Microsoft Taiwan Corporation, http://www.microsoft.com/taiwan/smallbusiness/issues/sgc/articles/select_sec_passwords.mspx

[2].Shih-Yung Chiang, The Implementation of Open Source Learning Management System Based on LDAP Distributed Authentication Architecture, National Yunlin University of Science & Technology Information Management-DEPT., 2004。

[3].School Free Soft，http://sfs.wpes.tcc.edu.tw/

[4].ChangKeng Lee, An Open Architecture for the Web-Based Single Sign-On Service, National Chiao Tung University Institute of Information Management, 2002.

[5].Chung-Huang Yang, Network Security:Theory and Practice, Taipei, Key Hold Information Inc., March, 2006

[6].Information and Instructional Technology Center,Kaohsiung City Government, http://www.kiec.kh.edu.tw/course/

[7].Gerald Carter, LDAP System Administration, O'Reilly, March 2003.

[8].IETF Internet-Drafts Database, https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=4718

[9].Ignacio Coupeau, Samba (v.3) PDC LDAP howto,http://www.unav.es/cti/ldap-smb/ldap-smb-3-howto.html

[10]. J´erˆome Tournier, Smbldap-tools User Manual, http://www.idealx.org/prj/samba/smbldap-tools.fr.html

[11]. J´erˆome Tournier, Olivier Lemaire, The Linux Samba-OpenLDAP Howto, http://www.idealx.org/prj/samba/smbldap-howto.fr.html

[12]. LDAPAccountManager, http://lam.sourceforge.net/

[13]. LDAPAccountManager I18N, http://lam.sourceforge.net/i18n/index.htm

[14]. McClure, Stuart, Scambray, Joel, FORGET BACKORIFICE:INVENTORY WINDOWS' SHARES AND ENFORCE PASSWORD POLICIES, InfoWorld, vol. 20, no.37 , 1998.

[15]. McClure, Stuart, Scambray, Joel, POORLY CHOSEN USER PASSWORDS CONSTITUTE MOST COMMON THREAT TO NETWORK SECURITY, InfoWorld, vol. 21, no.43, 1999

[16]. Moodle, http://moodle.org/

[17]. Open Webmail, http://openwebmail.org

[18]. phpLDAPadmin, http://phpldapadmin.sourceforge.net/

[19]. Tsung-Yi Tsai、Jia-Horng Wang、Wen-Nung Tsai, SMS – a Security Management System with LDAP, National Computer Symposium, 2005。

[20]. William Stallings, Cryptography and Network Security Principles and Practices(3 edition), Prentice Hall, Inc., August 27, 2002