以 WebDAV 整合 LDAP 與 SSL 建構安全簡便的校園網站維護系統

許文隆 楊中皇

國立高雄師範大學資訊教育研究所

allen66@ks.edu.tw chyang@computer.org

摘要

網頁製作與維護對於各級學校來說，已成為不可或缺的工作，不管是行政宣導，或是教學需求。但製作網頁，對於一般人來說，已有點困難度，再加上更新上傳網頁，需學習檔案上傳軟體或網頁製作發布軟體，實又增加使用者的阻礙。尤以目前入侵行為日炙，對於安全方面的考慮，資料實需有更安全的保障。本研究主要為建置安全簡便的校園網頁更新系統，目的為在安全性的考量下，讓學校老師或學生能以一般檔案存取狀態更新網頁。Server 端以 Linux 系統為平台，並使用 LDAP、SSL 與 apache 的 WebDAV 為服務協定，作為網頁之存取與安全保護技術。

在使用者端部分，為合乎使用者習慣，本研究以 PHP 程式建構 Web-Based 的使用者認證系統，讓使用者以一般瀏覽器方式通過認證登入系統，並將網頁空間連線成為電腦系統的網路磁碟機，使用者更新伺服器上的網頁就像在自己電腦更新一樣，讓網頁製作達到真正即時的『所見即所得』，建構出無時差，無痛苦的網頁維護環境。

關鍵詞：網路安全、網頁製作、SSL、LDAP、WebDAV

Abstract

In schools , they are very important jobs that edit and maintain web sites whether in administration or teaching. To design web pages isn't easy and they also need to learn upload applications. These works are difficult for teachers and students because they need to learn a lot of web applications. For that reasons, in this research we use LDAP、SSL and WebDAV in apache Linux server to design a simple and secure web update system that let everyone can upload their web pages easily.

In client we use php codes to design a Web-Based user authentication system that users can use browser to login the system and connect the web spaces to a network disk. Login users can design the web pages in that network disk just like in system hard disk. Therefore, they can maintain their web sites in "What You See Is What You Get" situation and construct a timeless and painless environment.

Keywords: Network Security、Web Edit、SSL、LDAP、WebDAV

1. 前言

隨著網際網路普植於眾人的生活中，在校園的應用也隨著需求呈現多元且差異化。目前，各級學校網管單位提供的網頁與檔案存取服務以網頁方式進行管理居多，目的是為了讓師生不用再學習一套應用程式—FTP。但部分也提供 FTP 服務，而對於沒有電腦基礎的老師或學生，使用 FTP 又成為一個很大的負擔。但以網頁存取的傳送檔案都有容量與數目的限制，所以當個別檔案內容很大或檔案數目繁多時，以網頁方式管理將成為消耗時間的夢魘。

因此本研究針對一般使用者網站維護與網頁檔案存取的需求，希望能在兼顧安全與方便之下，開發出一套安全的網站維護系統。伺服端以 Apache 模組的 WebDAV 協定來提供網路空間的服務，讓使用者可透過 http 連接埠來存取檔案。客戶端則以 Web-based 模式提供使用者登入介面，連線至伺服

器端的 LDAP 作使用者認證，再將網站空間連線成系統之磁碟機，以符合一般使用者使用習慣，建構出讓使用者在簡單安全的環境下，進行網頁維護工作，也可以當成網路磁碟機，進行檔案的存取工作。

2.文獻探討

本研究是以製作安全簡便的網站維護系統為主要目標，在伺服器端使用 WebDAV 的通訊協定，並安裝 OpenSSL 模組與 LDAP 加強網路使用者認證，減少帳號密碼遭盜取的可能，客戶端則以 PHP 開發使用者認證系統，並自動連結成網路磁碟機，茲將相關理論背景，分列以下說明：

2.1 WebDAV

WebDAV 的全名為『Web-based Distributed Authoring and Versioning』，中文譯為『Web 型分散式編寫和版本制訂』。WebDAV 允許使用者透過 HTTP 協定來存取與管理遠端檔案的網路協定標準。技術上來說是 http 通訊協定的一個延伸協定，其遵照 RFC2518 標準協定文件所建立，[12]利用 DAV 的前提是需要啟用相關模組與設定其權限。

WebDAV 是 HTTP/1.1 協定的延伸，增加了新的 HTTP 方法和標頭，支援任意類型的 Web 創作，不僅支援 HTML 和 XML，還支援文字、圖形、試算表以及所有其他格式[4]。

使用 WebDAV 可以完成的工作包括[8]：

- ●複合資料的操控。
- ●集合和資源管理。
- ●鎖定。您可以使用 WebDAV 禁止多人同時對一個文件進行操作
- ●名稱空間作業。您可以使用 WebDAV 方法 COPY 和 MOVE 讓伺服器複製和移動 Web 資源。

2.2 LDAP 輕量級目錄存取協定

LDAP 的全名為 Lightweight Directory Access Protocol，中文譯為『輕量級目錄存取協定』，為網際網路工程任務推動小組(Internet Engineering Task Force, IETF)標準之一(RFC2251)，最初係由美國密西根大學設計，可於 TCP/IP 通訊協定堆疊架構上工作，並由階層目錄中存取資訊[2]。透過 LDAP，使用者可於網際網路上輸入某些相關資訊，以尋找其它特定的資訊，例如我們可輸入某人的姓名、或是身份證字號，以尋找其電子郵件信箱或個人首頁網址等。經由共通之 LDAP，可將目前眾多的網路搜尋技術標準化，降低網路搜尋之紛擾[3]。本研究將導入 LDAP 作為使用者認證的機制，目前 WebDAV 模組使用的認證模式為普通密碼模式，其安全性尚稱不足，故使用 LDAP 加強使用者認證部分的安全控管，防止不當使用者入侵。

2.3 SSL 安全插座層

SSL 全名為 Secure Sockets Layer，中文一般稱為安全插座層。SSL 是由網景公司開發開發的安全開放標準，不但可以應用在網際網路（Internet）上，也可在全球資訊網（WWW）上的電子商務（EC）作安全把關，因為當初 SSL 開發的目的就是為了建立一個安全的通信通道，讓信用卡或金融卡等重要資訊不至遭到截取[1]。SSL 主要作用是在使用者傳輸資料之前先做加密處理，使資料變成亂碼，網站接收到資料之後再解密成原來的資料，這種方式沒有電子認證或者簽名，是目前網路上最被廣泛採用的一種規格[9]。

2.4 Web-Based Application

在網路尚未普及前，一般的公司行號或政府單位使用的軟體大多是 client-based 模式，也就是將軟體安裝在個人電腦上，用來執行各種工作與欲達成的目的。但隨著網際網路或是 Intranet 的普及，越來越多公司行號與行政單位採用 Web-Based 的軟體模式，也就是使用瀏覽器連線到伺服端，而不需要在個人電腦上進行安裝動作，即可進行相關的工作，這就是 Web-Based 的應用程式。而 Web-Based 應用程式有下列的好處[12]：

- ■ 跨平台。
- ■ 省成本。
- ■ 跨時空。
- ■ 高安全。

2.5 PHP 嵌入式編譯性語言

PHP 是一種伺服器端(server-side)與跨平台(cross-platform)的程式語言。通常以模組(module)的形式和 Apache 伺服器結合，並且提供多種連結資料庫的介面，如 MySQL，mSQL，PostgreSQL，Sybase，Informix，InterBase 等。目前 PHP 是屬於開放原始碼程式，遵守 GPL 的規定，可免費用於商業或非商業性質用途上，因此在世界各地的許多單位都有在使用[5]。PHP 的程式效能並不遜色於其他的同類伺服端介面語言如 iHTML， Cold Fusion，locomotive，JSP，ASP 等等，其執行效率和開發速率也比 Perl、C CGI 等快很多，本研究也因以上相關因素選擇 PHP 進行系統的開發。

3. 安全簡便的網站維護系統實作

3.1 系統架構

本研究所建立的系統概分為兩部分，一部分為伺服器端的安全管理與設定，另一部分為客戶端認證與安全的網頁更新系統的開發，其系統架構如下圖 1：

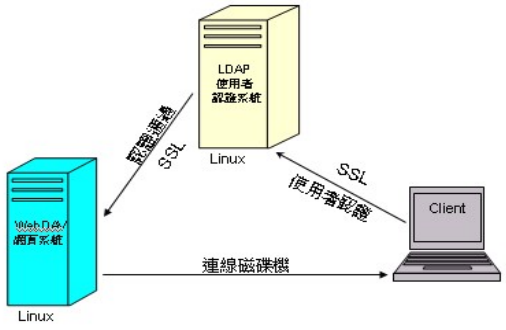

圖 1 網站更新系統架構圖

為建構整個系統，茲分以下三步驟，來完成整體研究：

一、安裝伺服器作業系統，以 Linux 作為系統平台，並啟用 http 服務與 webdav 功能。

二、在伺服器安裝 OpenSSL 安全模組，並且建立 LDAP 管理目錄建構使用者帳號密碼，來控制相關 http 服務的安全性與使用者的安全認證。

三、建構客戶端程式，採用 PHP 來開發，主要功能為連線 LDAP 驗證使用者的帳號與密碼，若驗證通過建立安全的網路連線磁碟機，讓使用者進行網頁更新。

3.2 伺服端的安全加強

伺服端以 Fedora core3 為作業系統，使用 Apache 2.0 提供 http 服務，並開啟 mod_dav 模組與 OpenSSL 模組，建立安全的網路傳送機制。並且安裝 LDAP 服務程式，建構安全的認證系統。

3.2.1 以 OpenSSL 進行安全連線

在目前封包竊聽盛行的時代，如何讓資料在傳送過程中不會遭受攔截與竊聽，是一件重要的工作。尤以在網頁模式下輸入帳號密碼，其被攔截的機會就更高。因此，本研究將管理帳號密碼的 PHP 網頁，全部以 https 執行，以免發生認證過程中帳號密碼被非法使用者竊取，這也是使用 OpenSSL 的主要因素。

OpenSSL 是一個開放原始碼的 SSL/TLS 連接埠套件，在安裝好 OpenSSL 之後，必須建立與管理一個 SSL 認證，並且要將 SSL 的 lib 模組寫入 apache 的設定檔中，讓 apache 可以執行 SSL。

3.2.2 LDAP 使用者帳號密碼的控管

電腦網絡經過長時間的發展，隨著使用者的增加，不同的操作系統和應用程式以各種的格式在網絡上存儲了大量的資料，對於網路管理者來說，為應付使用者使用不同的應用程式獲得不同的消息和資源，會造成系統很重的負擔。因此需要要一種新的技術，能夠以通用的格式和方式來達成資料儲存和共享，LDAP（Lightweight Directory Access Protocol）的出現，讓這種共享有個更進一步的實現。本研究以開放原始碼的 OpenLDAP 作為使用者帳號密碼認證，安裝 LDAP 之後，其可以獨立成單一的密碼認證伺服器，不只可讓本研究之網頁更新

程式使用，甚至整個單位的各種服務的密碼驗證，皆可連至本伺服器進行使用者認證工作。

安裝好 LDAP 之後，必須先行設定 ldap.conf 與 sladp.conf 兩個設定檔，接下來的工作最為重要，也就是建立使用者資料庫的部分，可以先建立一個資料庫資料夾：

mkdir davuser

進入該資料夾後，開始編輯使用者相關資料，該資料之編輯可以使用各種文字編輯器來編寫，但需依照格式來寫入使用者的相關資料。

編輯完之後，可以輸入下列指令，將使用者相關資料寫入 LDAP 伺服器中，其指令為：

ldapadd -D "cn=Manager, o= network.de" -w secret < /etc/openldap/ldif/datenbank.ldif

依照上列步驟，即可將使用者之相關資料輸入 LDAP 伺服器中，在應用程式需要驗證是否合法使用者時，即可進行認證的工作。

3.2.3 WebDAV 安全設定

apache 網頁伺服程式在安裝完後已經內建 mod_dav，該模組為提供 WebDAV 服務之模組，但預設是非啟動狀態，需要在 http.conf 內寫入啟動設定檔，並加入安全認證，管理可使用該服務之使用者權限。本研究之設定檔如下列，併列出解釋重要設定之涵義：

- DAVLockDB /tmp/DAVLock 為 DAV 模組其程式編寫或上傳時，存放暫存檔的地方。
- DAVMinTimeout 600 為連線逾期時間，以防長時間連線讓入侵者有機可乘。
- <Directory /home/*/www/> 到</Directory> 結束，為設定該發佈目錄權限的地方，例如本次為在/home/*/www 開始個別使用者的網頁空間目錄，作為檔案存取的地方。
- AuthName "Webdav" 為設定安全性時標題所顯示的名稱。
- AuthType Digest 以 digest 雜湊編碼模式作為登入時之安全性管理。
- AuthDigestFile /etc/httpd/dav.passwd 管理使用者密碼寫入的檔案。
- LDAP_Server 163.16.109.244 為連線 LDAP 伺服器的地方。LDAP 開頭皆為連線 LDAP 伺服器並讀取使用者相關資料，來進行驗證的動作。
- DAV On 開啟 dav 服務。
- AllowOverride None、 Options None 兩者為對於該資料夾相關權限所作的設定。
- <Limitexcept PUT POST DELETE PROPFIND PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>
  Require valid-user
  </Limitexcept>

此為最為重要的地方，為設定客戶端程式對於檔案之存取與權限使用的相關設定，Require valid-user 為須驗證帳號密碼方可使用 WebDAV 功能。

3.3 安全認證與使用便利的客戶端

本研究使用 PHP 開發客戶端的使用者介面，來提供使用者一個簡單好用的程式。使用者只需連線到相關網址，但網址是以『https://』開頭，以防帳號密碼被監聽與竊取。接著再輸入由管理單位給予的帳號密碼，經過簡單的認證手續，即可將伺服器網頁空間連線成網路磁碟機。(如圖 2)

圖 2：網頁更新系統頁面

對於使用者來說，連線網址與輸入帳號密碼是一個簡單的步驟，可是在系統運作中，卻進行的三道認證與連線手續，茲分述如下：

- 連線 Webdav 進行使用者認證：第一道使用者

認證為 Webdav 裡面經過 MD5 編碼的使用者認證，此認證為 Webdav 裡的基本安全使用認證。

- 比對 LDAP Server 使用者資料：接著 Webdav 會連線至 LDAP 伺服器，比對使用者身份是否符合規定，才能進行連線磁碟機動作。
- 連線網路磁碟機：當比對身分確認無誤，PHP 程式會執行連線網路磁碟機的動作，將個人的網頁空間連線成使用者端的網路磁碟機，可進行存取的動作。

而如果要進行網頁製作，使用者可以非常方便的將在編輯中的網頁存到網路磁碟機底下，然後使用瀏覽器連線到自己的網頁網址觀看，此不僅是網頁製作的『所見即所得』(What you get is what you see)，連上傳網頁也是同樣功能。如此，不管在教學上，或是教師製作網頁，都可以減少其工作步驟，增加使用效率與減低使用者障礙。(如圖 3.4.5)

圖 3：使用 FrontPage 編輯網頁

圖 4：直接將作好的網頁存於網路磁碟機

圖 5：使用瀏覽器直接觀看製作結果

最後，若是要將連線的網路磁碟機中斷，系統在連線時已經開啟一個新視窗網頁(如圖 6)，目的是為了讓使用者不要忘記將自己已經連線的網路磁碟機關閉。一般人在使用電腦後，若是公用電腦，若沒有關機，往往會將自己屬於個人資料的資訊留於之前使用的電腦。所以本系統在認證通過之後，會出現一個彈跳視窗，提醒使用者離開前不要忘記將自己的連線磁碟機中斷，以防資料遭竊或被破壞。當然，也可以使用系統預設的中斷連線網路磁碟機，只要在磁碟機上『按右鍵→中斷連線』即可。

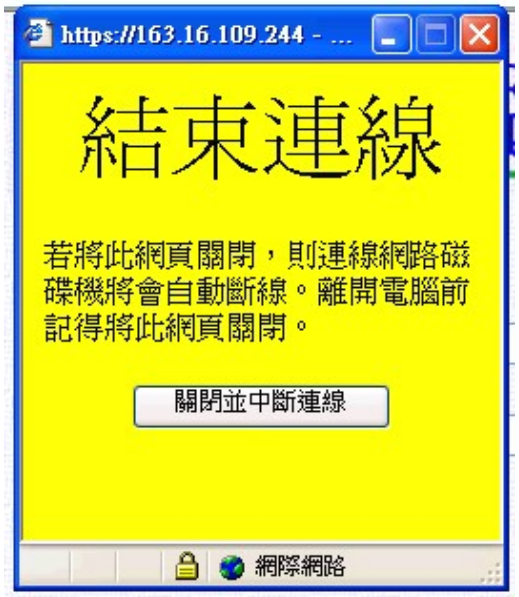

圖 6：系統連線後產生的提醒畫面

3.4 額外應用—網路隨身碟與取代 FTP

對於已經連線的網路磁碟機，除了應用於簡化網頁更新步驟外，更可以讓使用者當成隨身碟與檔案傳遞使用，我們可以稱之為『網路隨身碟』。對於資料的存取，就如同插入隨身碟一般，進行讀寫動作皆與一般使用隨身碟的方式一樣。所以，我們可以歸納出網路隨身碟的幾個優缺點：

- 不用隨身攜帶設備，有網路即可存取。相對的，當網路無法正常運作，其功能也就無法使用。
- 檔案大小可以隨時擴充，網路磁碟機之容量，可依照需求將使用者的 Quota 進行設定，目前硬碟非常便宜的情況下，要給予使用者幾 G 的容量並不是問題，減少隨身碟無法攜帶大檔案之限制。
- 傳輸速度依靠連線品質，若連線時與伺服器在同一網域，則其連線品質非常好，其速度甚至超過隨身碟的存取速度。但如果是在家中或使用上下傳不對等的 ADSL，則其存取過程中往往會有延遲的現象產生。

因此，連線的磁碟機，不管在更新網頁，或是存取需求的檔案，甚至進行資料備份，都是其可應用的範圍。

4. 結論

目前全國各國中小在進行擴大內需電腦的更新汰換，硬體更新後，相信會在資訊科技教學部分有更長足的進展。當然，除了硬體的更新，軟體與網路的應用也是重要的一環。隨著網路環境越趨蓬勃，如何讓使用者在『無痛』的環境中妥善應用網路資源，成為一個重要的課題。尤以校園中的莘莘學子，與教學業務繁重的老師，提供完善的網路應用與教學環境，讓『教』與『學』都可以無負擔的進行，實現九年一貫自然生活與科技領域的『資訊融入各科』的目標，讓資訊科技與網路在各科教學中都有所發揮與應用。

而本研究即針對此一目標而進行，尤以本研究所使用的伺服器應用程式皆是開放原始碼軟體，其安全性與經濟性都非常適合國中小來使用。當網路環境更普及與健全，簡化使用環境，使用者無須為某一功能而學習新軟體，其應用價值將更趨顯現，不管是簡化的網頁更新步驟，或是檔案傳輸與備份，都可將網路的應用效能再次提昇。

參考文獻

[1] 王百輝。使用 OpenSSL 實現安全的 FTP 伺服器。國立高雄第一科技大學通訊所論文。2004 年。

[2] 江世勇。LDAP 分散式認證架構下之開放原始碼教學網站建置與導入-以高職為例。雲林科技大學資管所碩士論文。2003。

[3] 安裝 LDAP 伺服器,http://www.linuxnetmag.com/cn/cnldap1.html。取得日期:2005 年 6 月。

[4] 林逸文、蘇秉豐。Linux 伺服器安全防護。2003。O’ REILLY。台北。

[5] 李蔚澤。Red Hat Linux 架站實務。2002。碁峰資訊股份有限公司。台北。

[6] 陳淑鈞、游原龍。數位證書登出及驗證之研究。2002。中華民國資訊通訊學會通訊第五卷第一期，pp.89-98。台北。

[7] 賴溪松、韓亮、張真誠。近代密碼學及其應用。2003。旗標出版股份有限公司。台北。

[8] 蔡明樹。以 XML 與 WebDAV 為基礎的網路教學系統。海洋大學系統工程所碩士論文。2001。

[9] 樊國楨、方仁威。電子簽章法及其應有之安全規範芻議。資訊安全論壇。，第五期，pp.20-35。2002。

[10] 經濟部技術處科專成果。LDAP 理論與技術。http://www.xml.org.tw/Function/Fglossary1.asp?key=LDAP。取得日期：2005 年 5 月。

[11] ITbase 資訊百科。SSL。 http://www.cnpedia.com/Result/Eword.Asp?Eword=Secure%20Sockets%20Layer%20(SSL)。 取得日期：2005 年 5 月。

[12] Fredj Dridi, Gustaf Neumann,”How to implement Web-based Groupware Systems based on WebDAV”, Proceedings of WETICE ’99, IEEE 8th Intl.1999.