SSL VPN 伺服器 OpenVPN 的安全設定考量

沈慧宇
服務單位 建國科技大學
電腦與通訊工程系
wyshen@ctu.edu.tw

黃文傑
服務單位 建國科技大學
電腦與通訊工程系
jay90042@gmail.com

莊展源
建國科技大學
電腦與通訊工程系
97410065@stu.ctu.edu.tw

摘要 —本文是針對 SSL VPN 的開放原始碼伺服器軟體 OpenVPN 的設定中，提出一安全設計的方式，特別是使用者端偽造 MAC address 所造成的阻絕服務攻擊，記憶體將因此完全耗盡，不僅導致 OpenVPN 伺服器無法運作，甚至可能使得整個作業系統必須重新開機，我們所提出的方法中會利用到 IP address 與 MAC address 結合對照關係表，如果違反這種對照關係表，不僅立即中斷連線，而且，用戶端的憑證也會被註銷，因此可以防止進一步的阻絕服務攻擊。

關鍵詞 - 阻絕服務、憑證、註銷

一、簡介

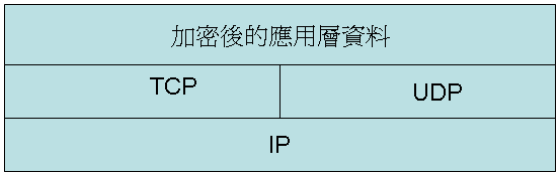
網際網路的資料傳輸雖然提供了極大的方便性，但是卻沒有辦法保證資料傳輸的安全性。早期為了解決這一個問題，大部分都轉向 ISP (Internet Service Provider) 業者租用專線 (leased line)，將安全性需求較高的資料傳輸線路獨立於網際網路之外，但是，租用專線的費用高昂，一般業者可能無法負擔，因此，VPN (Virtual Private Network) 的技術就因應而生。

VPN 原理主要包括建立通道 (tunneling)、加密傳輸 (encryption) 與認證功能 (authentication) 等三種技術，建立通道可以解決使用者端與伺服器端的路由問題，即使非 IP (Internet Protocol) 的封包資料一樣可以在網際網路上傳輸，例如 AppleTalk 或 NetBIOS 等通訊協定; 加密傳輸可以將明文 (plain text) 轉換成密文 (cipher text)，因此可以防止重要資料被洩漏; 認證功能則可以判定重要資料是否已被修改，換言之，加密傳輸可以避免被不當讀取，認證功能則可以避免被不當寫入。

目前網際網路上最主要的 VPN 技術大部份是以 IPSec (IP Security) [1]為主，IPSec 是作用在網路層 (Network Layer) 的通訊協定，它包括二種工作模式—傳輸模式與通道模式，每一種模式都包含二種通訊協定 AH (Authenticated Header)[2] 與 ESP (Encapsulated Security Payload)[3]。IPSec 可以提供完整的 VPN 功能，但是卻隱含許多缺點，第一，由於網路層的通訊協定功能是包含在作業系統內，因此，IPSec 的設計方式是依作業系統而定，換句話說，Windows 與 Linux 他們支援 IPSec 的方式將有所不同; 第二，AH 通訊協定所認證封包資料的範圍包括來源 IP 位址與目的 IP 位址，這樣的機制將使得 IPSec 無法通過防火牆，因為目前一般的防火牆都具有 NAT (Network Address Translation)的功能，而 NAT 勢必一定會更改來源 IP 位址與目的 IP 位址; 第三，IPSec VPN 的設定頗為複雜，這將使得 IPSec VPN 的應用不容易推廣。由於這三種缺點考量，本文所要探討的 VPN 安全設計將以 SSL VPN (Secure Socket Layer)為主，而不是 IPSec VPN。

有別於 IPSec VPN 是作用在網路層，SSL

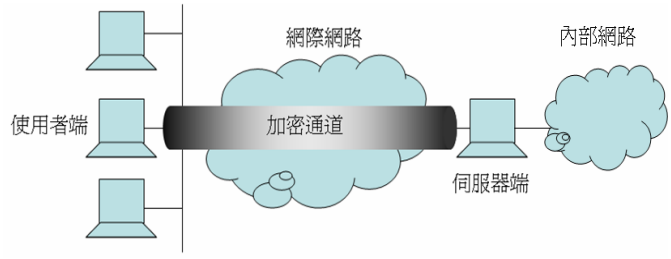
VPN 則是完全作用在應用層 (Application Layer)，如下圖一所示，OpenVPN 是實作 SSL VPN 的開放原始碼軟體，所以它可以適用於 Windows 與 Linux 二種作業系統，OpenVPN 的加密技術原理是以 SSL[4] 為基礎，它可以提供共享密鑰或公鑰系統二種加密機制，事實上，在加密機制這一方面，OpenVPN 很類似於 SSL，所不同的是 SSL 是以 HTTP (HyperText Transfer Protocol) 網頁存取為單一應用，但是，OpenVPN 則可以適用各種不同的應用層通訊協定，因此，非常適合運用於網際網路。



圖一 SSL VPN 的 OSI 功能層

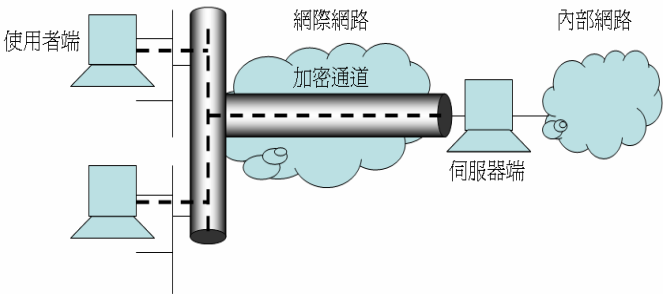
二、系統架構

我們所採用的作業系統是 Fedora 10 Linux[5]，伺服器軟體是 OpenVPN 2.0.9[6]，使用者端作業系統則以 Windows XP 為主。OpenVPN 包括橋接模式 (bridged mode) 與路由模式 (routed mode) 二種操作模式，由於本文所要解決偽造 MAC address 的攻擊方式是以橋接模式為主，因此，所有使用者端與伺服器端都要在設定檔內寫入 dev tap 參數 (路由模式則是寫入 dev tun 參數)，整個 OpenVPN 運作系統架構如下圖二所示。



圖二 系統架構

在橋接模式下，所有使用者端與伺服器端都是處在一個虛擬的區域網路，換言之，他們都會存在同一個虛擬網段，如下圖三所示，所有主機都可以接收廣播封包，所以，包括 Windows 的網路芳鄰，或甚至非 IP 通訊協定的封包，都可以提供很方便的應用，而事實上，這也正是本文希望以橋接模式為討論主軸的原因，然而，如果駭客出現在此虛擬網段，卻無形中存在被攻擊的危險。



圖三 橋接模式架構

三、系統功能與運作原理

（一）認證程序

由於 SSL 互動程序 (SSL Handshaking) 耗費很多 CPU 運算資源，為了避免攻擊者產生大量錯誤的連線請求，導致 OpenVPN 陷入無謂的運算迴圈，因此，基於安全考量，我們建議在伺服器端與用戶端的設定檔中各加入以下參數

tls-auth dos.txt 0　　(OpenVPN 伺服器端)，
tls-auth dos.txt 1　　(OpenVPN 使用者端)，

dos.txt 是一個使用者端與伺服器端所共享的檔案，所以必須以另外的安全通道 (例如 SSH) 傳送到所有使用者端的主機，他是由以下指令所產生

openvpn –genkey –secret dos.txt，

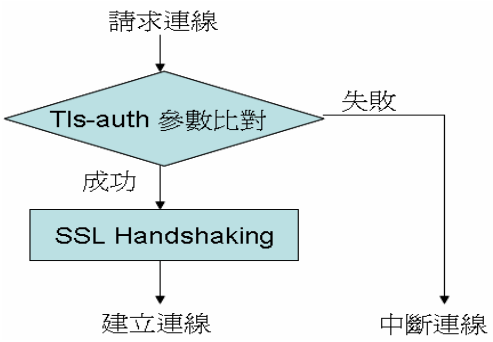
上述指令所產生的 dos.txt 檔案不僅可以搭

配 tls-auth 參數設定，而且，如果不是採用公鑰的加密系統，而是採用最簡便的共享密鑰加密方式，則 dos.txt 可以做為雙方的共享密鑰 (shared key) ，其設定方式如下

secret dos.txt (OpenVPN 伺服器端)，

secret dos.txt (OpenVPN 使用者端)，

透過 dos.txt 的設計，如果無法通過認證程序，後續的 SSL 互動程序就不會被執行，如下圖四所示，進而避免了伺服器端寶貴的運算資源，所以 tls-auth 參數可以算是 OpenVPN 的一道防火牆。



圖四 tls-auth 執行流程

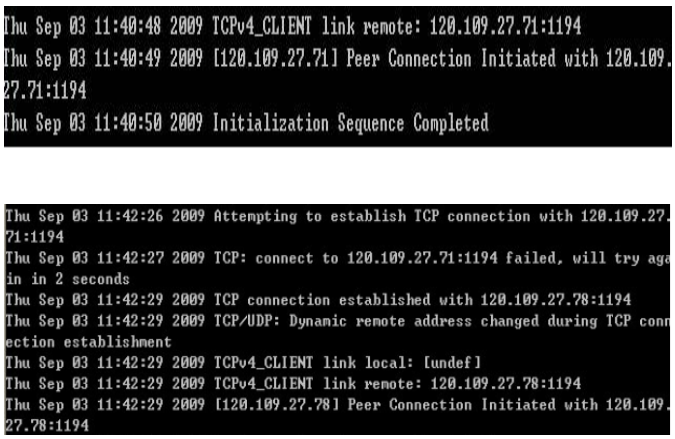
（二）平衡負載與容錯 (failover) 設計

由於 OpenVPN 是以一般使用者程序在執行，而且許多加密與解密過程非常耗費 CPU 運算，所以，遇到大量連線需求時，OpenVPN 伺服器的效能自然大受影響，因此我們建議 OpenVPN 伺服器不止建置一台，平常多台伺服器可以共同分擔網路流量，但是，當某一台 OpenVPN 伺服器當機時，新的連線請求就會切換到正常運作的 OpenVPN 伺服器上。

使用者端的 OpenVPN設定檔參數寫入如下

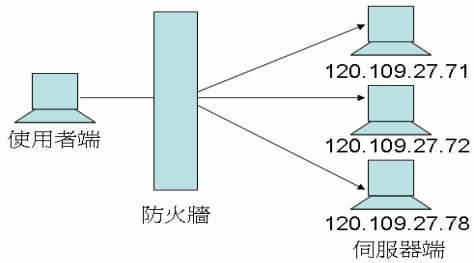
remote 120.109.27.71 1194
remote 120.109.27.70 1194
remote 120.109.27.78 1194
remote-random，

上述範例共有三台伺服器參與運作，不同的使用者會隨機挑選一台 OpenVPN 伺服器發出連線請求，因此，在常態分佈的假設下，伺服器可以平均負擔不同使用者的網路流量。值得注意的是，停止運作的 OpenVPN 伺服器並不會加入被挑選的行列，在下圖五中，我們可以發現當 120.109.27.71 斷線後，使用者會自動切換到另一伺服器 120.109.27.78，新的連線可以重新建立起來，所以可完成容錯的設計。



圖五 OpenVPN 伺服器切換連線請求

另外，我們也可以透過 iptables 防火牆軟體來切換挑選適當的伺服器端主機，這樣就可以在伺服器端控制平衡負載的動作，如下圖六所示，而不是由使用者端決定是否須要平衡負載與容錯的設定，只是這一部份的相關設定並不屬於 OpenVPN 的功能，因此，本文未擬贅述其詳細設定。



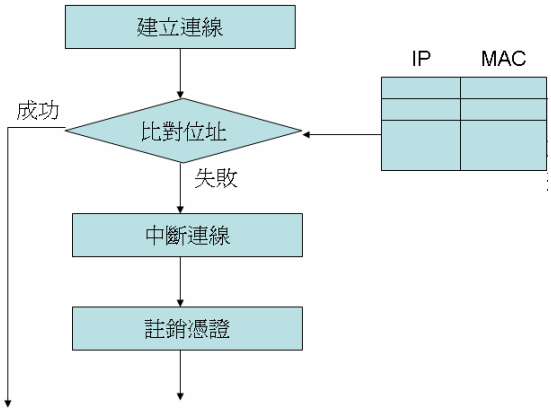
圖六 OpenVPN 與前端的防火牆

（三）阻絕服務

DoS (Denial of Service) 阻絕服務攻擊最大的特色是耗盡伺服器端主機的資源，這些資源可能包括網路頻寬、CPU 運算、記憶體容量、與硬碟空間等，一旦資源耗盡，伺服器端主機就無法再提供任何正常的網路連線。在橋接模式的運作下，攻擊者若是可以通過正確的認證程序 (本文主要是研究阻絕服務攻擊，並沒有探討攻擊者如何通過正確的認證程序)，他可以產生大量的網路封包流量，而且每一個網路封包的來源 MAC address 都是偽造的，這將造成 OpenVPN 忙於許多無意義的計算，並耗盡所有虛擬記憶體 (因為 OpenVPN 不是屬於核心程式)。

OpenVPN 伺服器端的設定檔提供了一個很有用的參數 client-connect detect.sh，detect.sh 是我們所設計的程式，使用者連線一旦成功建立，client-connect 參數會要求 OpenVPN 立刻執行 detect.sh 程式，在 detect.sh 程式中，IP address 與 MAC address 的比對關係會被建立並做為後續的比對基礎，若是比對失敗，則中斷使用者端與伺服器端的連線，並註銷 (revoke) 使用者的憑證，以中止未來 SSL 互動程序，關於註銷憑證方面，OpenVPN 軟體已提供註銷使用者的憑證所需要的相關執行檔案，OpenVPN 可以記錄哪些使用者的憑證已被註銷，下圖七則表示 detect.sh 的執行流程圖。

另外，我們還須搭配另一伺服器端的設定參數 learn-address addr.sh，learn-address 主要是用來驗證使用者端在安全通道中的虛擬 IP address 的正確性，因此，在 addr.sh 程式中，我們可以決定是否要新增、刪除或修改所學習到的 MAC address 或 IP address，再透過 MAC address 與使用者憑證上 Common Name 的關聯性，可以進一步判斷出是否某一使用者正產生大量不同 MAC address 的網路封包。



圖七　detect.sh　功能方塊圖

四、討論

本文主要研究 OpenVPN 伺服器建置過程中安全性的設定考量，他們包括認證程序、容錯設計與阻絕服務的攻擊，我們相信這些設定與討論將有助於建構更安全穩健的 VPN 伺服器網路系統。

我們特別希望更進一步說明的是 detect.sh 程式的功能，因為，它的存在作用還可以防範其他類型的攻擊。

關於偽造 MAC address 所造成的阻絕服務攻擊，OpenVPN 的官方網站 [7] 在目前 2.0.9 最新版本中已提出一解決方案，他利用一個新的參數設定 max-routes-per-client 以限制每一用戶端最大的路由總數 (每一用戶端連線都對應一個路由表格)，但是，我們認為 detect.sh 不僅可以偵測出 MAC address 的改變，而且，detect.sh 也具有認證使用者端網路卡的意義。

事實上，在一般區域網路中，IP address 結合 MAC address 的比對功能是非常平常且必要的，因為，攻擊者偽造 MAC address 的目的常常並不僅止於阻絕服務的攻擊，而且，也正因為橋接模式的功能就是在模擬區域網路，所以，攻擊者甚至可以將受駭主機的 MAC address 更改為區域網路上其他電腦的 MAC address，以攔截

其他電腦的網路封包資料，而遂行更進一步的攻擊。然而，max-routes-per-client 參數設定卻僅能避免阻絕服務的攻擊。

五、參考文獻

[1] IPSec: http://www.ietf.org/rfc/rfc2401.txt

[2] AH : http:// www.ietf.org/rfc/rfc2402.txt

[3] ESP: http:// www.ietf.org/rfc/rfc4303.txt

[4] SSL: http://www.ietf.org/rfc/rfc2246.txt.

[5] Fedora: http://fedoraproject.org/

[6] OpenVPN: http://www.openvpn.net/

[7] Changelog:http://www.openvpn.net/index.php/open-source/documentation/change-log/71-21-change-log.html