Linux 環境下以 AES 及 SHA-256 強化 VPN 的設計與實現

翁木龍、楊中皇
國立高雄第一科技大學資訊管理系（所）
E-mail：u8924816@cc.nkfust.edu.tw 、chyang@computer.org
蔡瑞明
Business Computer Information Systems Department, Saint Cloud State University
rjtsai@stcloudstate.edu

摘要

在Internet上安全的通信一直是組織及個人都非常重視的一環，對於安全性的高度需求造成一股VPN的風潮。IETF制定的IPSec協定組是VPN中應用最廣泛的一個開放標準，而FreeS/WAN是在linux、freebsd平臺下對IPSec的實作。本文試圖透過對FreeS/WAN開放原始碼（open source code）的研究，提出將AES-128及SHA-256加入FreeS/WAN中的原則及實做，並配合低成本的硬體設備，使得經由FreeS/WAN設定的IPSec通信環境更有效率及更安全。

關鍵字：AES、FreeS/WAN 、IPSec、SHA、VPN

壹、研究動機與目的

目前國內有關IPSec的論文，在全國博碩士論文中可查到的有「降低叢集架構式IPSec閘道之封包失序現象」，內容為調整在叢集架構式IPSec閘道中防封包重送機制（Anti-Replay Window），進而降低封包失序所帶來的影響 [1]。及「在VPN路由器中設計並實作IPSEC」[2]、「在VPN路由器上設計並實作IKE」[3]，分別是將現有的TCP/IP架構中加入此IPSec及IKE的模組。此外還有「利用IPSEC達成封包傳輸隱匿之目的」[4]，利用IPSEC的機制設計了一個加強的模式，並利用Security Gateway的功能，將Source Routing所需的IP Address做加密處理來達到隱藏傳輸路徑的目的。而目前工研院電通所開發完成IP-VPN閘道器，已通過美國ICSA認證，其中即具備IPSec功能。

一、研究動機

1.了解網路通信上的安全威脅

目前網路安全威脅的種類，約可分為以下數種[5]：

(1)IP spoofing：駭客偽造 Ip address。
(2)Session Hijacking：駭客打斷原先用戶端連結，模擬成用戶，竊取資料。
(3)Eaversdropping：竊聽、竄改資料。
(4)Man-in-the-Middle：攻擊者同時冒充A與B通信，冒充B與A通信。
(5)Clogging：被攻擊者花大量系統資源在Key的計算上，使正常服務效率變差。
(6)Replay attack：造成DOS（Deny of service），阻礙正常服務的進行。

2.探討 VPN 的實作過程

目前很多廠商都提出VPN的實作（implement），但大多是屬於黑箱作業，外人無從知悉內部的運作，而FreeS/WAN具有開放原始碼的特性，正可彌補這個缺憾。

3.應用新的演算法

經由對新演算法的研究與應用，可對較先進的理論多一份瞭解。

二、研究目的

應用AES及SHA-256強化VPN的功能，使VPN通信環境更有效率及更安全。

貳、VPN 提供的解決方案

Paul Ferguson and Geoff Huston曾提出VPN定義如下：「A VPN is a private network constructed within a public network infrastructure， such as the global Internet.」[6]，也就是說VPN是在一種讓公共網路（例如Internet）變成像是內部專線網路的方法。

為何企業界會熱衷使用VPN呢？主要是使用VPN有以下的優點：節省企業長途電話通訊成本、節省企業長途專線通訊成本、具有彈性，容易擴展、精簡設備需求，裝置非常容易，節省企業維護網路人事成本。

而目前常用的VPN標準，約有以下三種：[7]

1.PPTP (Point-to-point Tunneling Protocol)

PPTP (點對點隧道協議)是PPP(點到點協議)的擴充，屬於第二層的隧道傳輸技術。支援該協定的公司包括Microsoft 、Ascend Communications、3Com/Primary Access、ECI Telematics和US Robotics等，目前仍屬於draft階段。PPTP 的最大優點是Microsoft的支援，因為Windows作業系統都內建PPTP ，另一優點則是可支援IP/IPX/NetBEUI 等通訊協定。缺點是PPTP 只能執行點對點VPN的功能，無法同時執行Internet 的應用，使用時較不方便。還有另一缺點就是安全問題，在PPTP draft中只利用PPP的驗證功能來確保安全，但是Microsoft在這方面已有所改進（使用MPPE及EAP協定）。採用這種方案時，PPTP協定軟體必須運行在Windows 作業系統工作站上。

2.L2TP (Layer 2 Transport Protocol)

L2TP是PPTP、 L2F兩個較早期的協議擷取優點相結合成的結果，主要由Cisco發展。L2TP的優點是能提供高效率的連線服務、能支援多種傳輸協議、提供端點之間的身份認證（PPTP只提供使者的身份認證），但是它沒有提供很好安全保護措施。例如:L2TP本身不提供任何加密方法，當資料需要保密時，就要要依賴別的協定（如IPSec）。

由於有一些安全問題，IETF的本來有一些成員提議將PPTP和L2TP發展類似的ISPec的協議，但是又考慮到ISPec已經日漸成熟，因此，IETF決定使用已有的IPSec協議來為L2TP通道提供安全保護。

3.IPsec (Internet Protocol Security) [8]

IPsec是IETF 所制定的業界標準，可以提供 Internet 、Intranet 、Extranet 和Remote Access，是IPv6 的必須實做的標準之一（在IPv4則是option）。IPSec只提供基礎架構，因此很容易套入新的演算法，非常具有彈性，其次是具備透通性，使用者不需更新應用程式即可使用，由於優點很多，是未來VPN應用的主流。

IPSec 是設計來達到網路層（network layer）中端對端安全通訊，主要有三個大協定：ESP 、AH 、IKE，其 中 ESP(Encapsulation Security Payload) ：提供認證和加密。AH(Authentication Header)：只提供認證的動作，通常是靠MD5 、SHA1 、HMAC 來確認使用者的身分。IKE：使自動交換密鑰，產生的密鑰可用來加密及認證。

上述VPN標準，其中以IPSEC使用最廣泛。

參、IPSEC 標準

IPSec 提供了一種標準、安全以及具有彈性的機制，可用來？IP及上層

協定（如UDP和TCP）提供安全的保證。IPSec ？了保障I P 資料封包的安全，定義了一套特殊的方法，規定了要保護的是什？樣的通信（traffic）、如何保護以及身分驗證。IPSec本身也定義了一套預設的的演算法，以確保不同的實做方案相互之間能具備互通性。如果想增加新的演算法，過程非常容易，並不會破壞互通性。總之，IPSec 可保障主機之間、網路安全閘道（network security gateway如路由器或防火牆）之間或主機與安全閘道之間的資料封包安全。

一、IPSec 架構[9]

IPSec 協定主要包括下列元件：AH （Authentication Header）、ESP（Encapsulation Security Payload）、IKE（Internet Key Exchange）、ISAKMP / Oakley（IKE） 以及Transform Method（加密或認證演算法）。這些元件之間的關係可用下圖來表示：

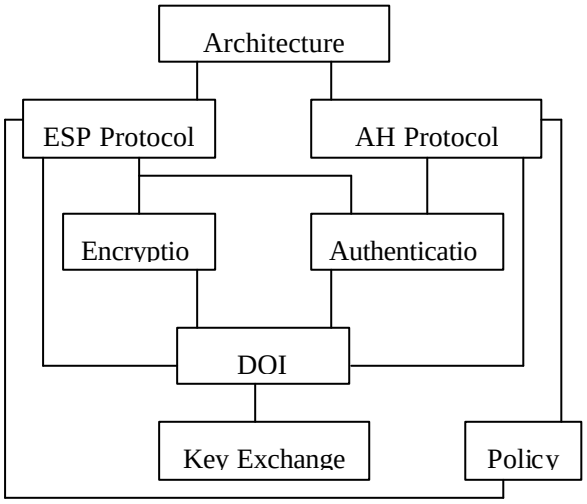

圖1： IPSec體系（摘錄自[10]）

IPSec可使用ESP （Encapsulation Security Payload）、AH （Authentication Header）這兩個協定來保障安全通信，ESP可？IP封包提供機密性、資料來源身份認證、抗重送攻擊以及資料完整性等安全服務。AH可？I P封包提供資料完整性、資料原始身份認證和抗重送攻擊等安全服務。其中ESP有加密及認證演算法，而AH只有認證演算法。IKE （Internet Key Exchange）用來協商通雙方，？IPSec產生密鑰。而協商時使用的參數則被歸類在一個單獨的文件中，名？IPSec DOI（Domain of Interpretation）[11]。目前尚未成？標準的一個重要元件是“策略”（Policy）。策略是一個非常重要的問題，因？它決定兩個實體之間是否能夠通信；如果能的話，要採用哪一種轉碼方式（Transform Method）。如果策略定義不當，可能導致雙方不能正常通信。

二 IPSec 模式[12] [13]

IPSec的模式和協定共有四種組合：也就是AH的Transport Mode（可譯為傳送模式）、AH的Tunnel Mode（可譯為通道模式）、ESP的Transport Mode以及ESP的Tunnel Mode。但在實際應用中，我們並不採用 AH 的 Tunnel Mode，因？它保護的資料與AH的Transport Mode保護的資料是一樣的，而且大部分IPSec Tunnel Mode的實做都希望具有機密性，因此大多會採用ESP。AH 和ESP 標頭在Transport Mode 和 Tunnel Mode 之中都不會改變。兩種模式的區別非常直觀，它們保護的東西不同，一個是I P 整個封包，一個是I P Payload。詳見圖2及圖3。

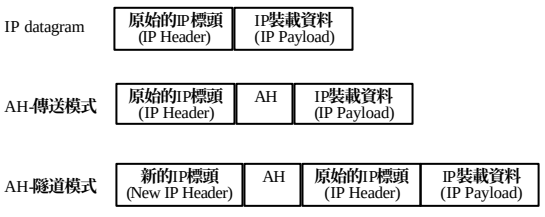

圖2 AH的操作模式（IPv4）

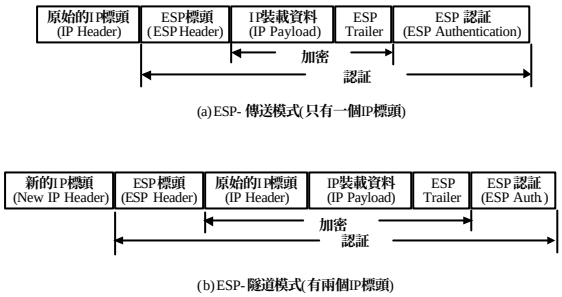

圖3 ESP的操作模式（IPv4）

三、安全聯盟[14]

Security Association（簡稱SA 安全參數組合）是IPSec 很重要的基礎。SA 是兩個通信實體經協商建立起來的一種協定。SA決定了用來保護資料封包安全的IPSec 協定、加密方式、密鑰值、密鑰長度以及密鑰的有效存在時間等。任何IPSec 實施方案都會構建一個SA資料庫（簡稱SADB Security Association Database），由SADB來維護IPSec用來保障資料封包安全的一些資訊。

SA是單向的。因此如果兩個主機（比如A和B）正在通過ESP 進行安全通信，那？主機A 就需要有一個SA，即SA_A (out)，被用來處理外出的資料封包；但還需要有另一個不同的SA，即SA_A (in)，用來處理進入的資料封包。主機A的SA_A (out)和主機B的SA_B (in)將會有相同的加密參數（比如說相同的密鑰）。同樣的，主機A的SA_A (in)和主機B的SA_B (out)也會共用相同的加密參數。由於SA是單向的，所以針對外出和進入處理使用的SA，都分別需要維護一份單獨的資料表。

此外，每種協定都有一個SA 。如果主機A和B同時通過AH和ESP進行安全通信，那？每個主機都會針對每一種協定來構建一個獨立的SA，亦即有AH外出和進入處理使用的SA，及ESP外出和進入處理使用的SA，共需要建立四個SA。

若安全策略要求？兩個主機建立多個SA，以便進行安全通信，那？這些SA的集合便稱？SA bundles。

IPSec 體系中有另一個元件，稱？Security Policy Database（簡稱SPD 安全策略資料庫）。在IPSec封包處理過程中，SPD 和SADB 這兩個資料庫需要聯合使用。策略是IPSec 結構中一個相當重要的元件。它定義了兩個實體之間的安全通信特性；定義了在什？模式下使用什？協定；還定義了如何處理IP封包，每個SPD都有一個pointer指向SA或SA bundles。此外在密鑰的交換上有自動[15]及人工兩種。

肆、以 FreeS/WAN 建立 IPSEC VPN

FreeS/WAN[16]是在 linux、freebsd平臺下對IPSec的實作。選擇FreeS/WAN最主要一點是FreeS/WAN是免費的(而Linux也可以免費取得)，且有完整的原始碼。而就目前的市面上商業或是其它免費VPN應用方案來看， FreeS/WAN被越來越多的軟硬體VPN使用，互相操作性很好。目前LInux有一個LRP(linux router project)專案，強調用一片磁片或一片CD-ROM開機後，可將一般的PC做成router，該router就成為一部Security Gateway，其中使用到的VPN程式即為FreeS/WAN。目前FreeS/WAN被包含在以下的Linux distribution：European versions of SuSE Linux (Germany)、Conectiva (Brazil)、the Polish(ed) Linux Distribution (Poland) 、 Mandrake (France)、Debian。由於密碼出口管制的原因，美國輸出Linux distribution不可包含FreeS/WAN。

在安裝方面，FreeS/WAN的官方網站www.freeswan.org上有完整的安裝介紹。也有人提供Webmin介面的安裝程式module（http://www.niemueller.de/webmin/modules/freeswan/），可使安裝更為便捷。

目前FreeS/WAN 1.95版幾乎支援了大多數的RFC IPSec標準，因此具備

了所有IPSec的功能。在互相操作性（interoperation）上，根據FreeS/WAN小組的測試，也可和大多數VPN設備互通。FreeS/WAN採用的是：IPSec以模組的形式插入到鏈路層、IP層、TCP層之間），而不是採用IP與IPSec結合的實現方式。

伍、在 IPSEC 上實作 AES 及 HMAC-SHA-256

一、AES 概述

美國全國科學與技術委員會（NIST National Institute of Science and Technology）在2001年正式宣佈AES（Advanced Encryption Standard）成？新聯邦資訊處理標準FIPS-197(FIPS--Federal Information Processing Standard)。AES將用於美國政府組織保護敏感資訊的加密演算法，而且未來也會廣泛地應用在公司組織、學校及個人資料通訊上。由於DES在一天之內即可被破解，預料AES被將會取代DES。但NIST認為Triple DES在未來一段時間內仍會被使用。

經過四年的嚴格評選，NIST從眾多演算法中選擇Rijndael為AES的標準。Rijndael在軟硬體的運算測試環境中，都一直表現非常出色，有很好的靈活性。

二、將 AES 應用在 IPSec

Triple DES雖然夠安全，但仍有一些缺點存在，而且加解密速度都需要較長的時間。由於AES的運算速度及安全性都比Triple DES好，而且可免費使用（不管使用者是什麼目的），沒有出口限制的問題。因此一般認為未來IETF IPsec Working Group將會採用AES作為Ipsec的預設加密法。目前已有一份RFC草案The AES Cipher Algorithm and Its Use With IPsec，提出將AES應用在IPSec的方法。草案大致的要點如下：[17]

1. Mode：目前FreeS/WAN上使用的加解密mode是CBC（Cipher Block Chaining）。雖然尚未定義操作IPSec使用AES的mode，但由於CBC mode 是一個定義良好且易於瞭解的對稱式加密mode，而且被大多數ESP加密所採用。因此草案中認為可在ESP加密時使用CBC mode（AES cipher in CBC mode）。而CBC所需要的Initialization Vector (IV)，則和加密區塊大小相同。IV是經由亂數隨機產生。[18]
2. Key Size：AES預設的 key size 是128 bits 。在FreeS/WAN（IPSec）中參與通信的每一邊都會生成四種密鑰：分別是一、SKEYID，其他三個密鑰都以它做基礎；二、SKEYID_d，作為產生出密鑰的材料（material）；三、SKEYID_a ，用來保障資料的完整性及對資料來源的身份進行驗證；四、SKEYID_e，用於加密演算法的密鑰。這四個密鑰都是以PRF（Pseudo Random Function）函數的方式產生，PRF通常都是兩邊協商好的某一個HMAC函數。因此這個HMAC函數區塊長度決定了四個密鑰的長度。假如PRF的輸出位元數太少或太多，不能作？一個加密或認證的密鑰來使用，那？就必須進行擴展或裁減，直到達到位數的要求？止。在原先Triple DES中Key Size是64 bits，在AES則為128 bits。
3. Block Size：加密區塊大小16 octets (128 bits)，由於要維持128 bits的區塊大小，因此必要時要做Padding處理。
4. Rounds：依照AES的規格，128-bit keysize，要執行10 次rounds。這一部分在加解密程式中會定義。
5. ESP payload 修改：由於ESP payload中有一IV的欄位，必須修改成和區塊大小相同（128 bits）。在原先Triple DES中的欄位長度都是32 bits的倍數，因此應修改如下圖：

Initialization Vector (16 octets)
Encrypted Payload (variable length， a multiple of 16 octets)

圖4 ESP payload修改的欄位長度

IANA設定Encryption Algorithm ID為7 給AES-CBC。也設定給ESP Transform ID為12 給 ESP_AES。

三、HMAC-SHA-256 概述

HMAC是密鑰認證的機制（keyed authentication mechanism），保證封包被認證且未被修改。它利用密碼學中的雜湊涵數如MD5、SHA-1等與一把金鑰(Secret Key)一起運算產生摘要(Digest)，藉由比對摘要的值，通信雙方可以查出資料在處理或傳輸過程中是否保持完整。

HMAC-SHA-256 是 SHA-256 和 HMAC 的結合。可提供較大的Block size（512 bits）和較大的Hash長度（256 bits），因此安全性較高。

四、將 HMAC-SHA-256 應用在 IPSec

RFC 草案 The HMAC-SHA-256-96 Algorithm and Its Use With IPsec，提出將HMAC-SHA-256使用在ESP和AH的認證作業。要點概述如下：[19]

1. Keying Material：應該使用較強（strong）的 pseudo-random function 來產生 256-bit key。FreeS/WAN用SKEYID_a作為Keying Material。
2. Padding：依照目前SHA2-1的草案來看，並不需要增加額外的padding。
3. Truncation：只使用前面的96 bits，配合ESP payload。[20]

IANA 已經設 identifier Hash Algorithm ID為4給SHA2-256。設identifier AH Transform ID為5 給AH_SHA2-256 。 設 AH/ESP Authentication Attribute Value為5 給HMAC- SHA2-256。

五、認證密鑰管理

RFC 2409中提出四種身分認證的方法，分別是pre-shared key、digital signature 、 public-key 、 revised public-key。 在 FreeS/WAN 中支援 pre-shared key及RSA-signature兩種方式。本研究是將pre-shared key放在IC卡這種低成本硬體設備中，當需要時再由硬體裝置讀出，如此可進一步確保VPN的整體安全性及易於管理。安裝於Linux環境下的FreeS/WAN形成secure gateway (SG)，經由網際網路與另一端的SG之間便可以IPSec保障通信的安全。FC 2409中提出四種身分認證的方法，而在FreeS/WAN中支援Pre-shared key及RSA-Signatur兩種方式。本研究初步構想是將Pre-shared key或RSA的private key放在smart card中，當需要時再由smart card reader讀出，如圖5，如此可進一步確保VPN的整體安全性。

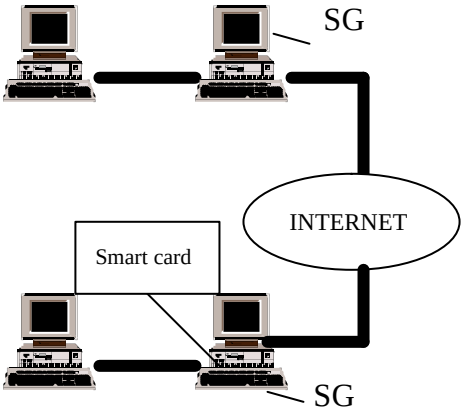

圖5 本研究硬體架構

目前將Key放在IC卡產品有SSH Communications Security Corp，該公司宣稱將Key放在IC卡中，並用來做為認證及auto config VPN設定，這是該產品的一大特性。

陸、結論

本文提出修改FreeS/WAN原本的加解密及認證演算法，所應注意的原則，這些原則目前已有RFC草案提出，預計不久將會成為標準，使用類似FreeS/WAN這些open source的軟體，可讓使用者可依照自己的需求來改善原本的功能，再搭配上低成本的硬體設備使得密鑰管理更完善，將可使開發新系統更具彈性及安全性。

致謝

本研究部分成果承蒙國科會計畫（NSC 90-2213-E -327-008）的經費補助，特此致謝。

參考文獻

1. 許勝凱（2000），“降低叢集架構式 IPSec 閘道之封包失序現象”，國立交通大學碩士論文
2. 應中龍（2001），“在 VPN 路由器中設計並實作 IPSEC”， 大同大學碩士論文
3. 林育德（2001）， “在 VPN 路由器上設計並實作 IKE”，大同大學碩士論文
4. 高笙庭（2000）， “利用 IPSEC 達成封包傳輸隱匿之目的”，臺灣大學碩士論文
5. Alcatel Networks Corp.（2000），“Understanding the IPSec Protocol Suite ” http://www.alcatel.com/
6. Paul Ferguson and Geoff Huston （1998）， “What is a VPN? ”， http://www.employees.org/~ferguson/vpn.pdf
7. Casey Wilson, Peter Doak （ 1999 ） ， “Creating and Implementing Virtual Private Networks: The All-encompassing Resource for Implementing VPNs”， The Coriolis Group
8. S. Kent and R. Atkinson（1998），“Security Architecture for the Internet Protocol”， RFC2401，IETF
9. R. Thayer（1998），N. Doraswamy and R. Glenn， “IP Security Document Roadmap” ， RFC2411，IETF
10. Naganand Doraswamy， Dan Harkins（1999），“Ipsec: The New Security Standard for the Internet，Intranets， and Virtual Private Networks”，Prentice Hall PTR
11. D. Piper（1998）， “The Internet IP Security Domain of Interpretation for ISAKMP”， RFC2407，IETF
12. S. Kent and R. Atkinson（1998），“IP Authentication Header”， RFC2402， IETF
13. S. Kent and R. Atkinson（1998），“IP Encapsulating Security Payload”，RFC2406，IETF
14. D. Maughan， M. Schertler （1998）， M. Schneider and J. Turner， “Internet Security Association and Key Management Protocol”， RFC2408，IETF
15. D. Harkins， D. Carrel（1998），“The Internet Key Exchange (IKE)”，RFC 2409，IETF
16. FreeS/WAN official Home Page，http://www.freeswan.org/
17. C. Madson and N. Doraswamy （1998）， “The ESP DES-CBC Cipher Algorithm With Explicit IV”， RFC2405， IETF
18. S. Frankel，S. Kelly（2001），“The AES Cipher Algorithm and Its Use With IPsec”， Internet Draft ， IETF
19. S. Frankel，S. Kelly（2001），“The HMAC-SHA-256-96 Algorithm and Its Use With IPsec” ，Internet Draft ，IETF
20. C. Madson and N. Doraswamy （ 1998 ） ， “The Use of HMAC-SHA-1-96 within ESP and

AH”， RFC2404， IETF