結合 IC 卡與 PKI 的 IPv6 安全機制設計與實現

翁木龍，中華電信訓練所

楊中皇，高雄師範大學資訊教育研究所

摘要

原始 IPv4 的設計架構中並未考慮到安全的問題。而下一代的 IPv6 為了加強通訊資料的保護，內建了 IP Security（簡稱 IPSec）的安全機制。IPSec 根據通信雙方的安全政策，決定通信時是否要對資料加以保護，並可使用 IKE（Internet Key Exchange）協定自動交換密鑰，以驗證身分並產生加密及認證的密鑰。IKE 協定將代表身分的 Key 確認無誤後，才進行 AH（Authentication Header）或 ESP（Encapsulated Security Payload）的認證或加密服務。IC 卡被認為是儲存數位資料最安全的媒體，而 PKI 所發的憑證，具備結合個人身分及公鑰的公信力，本研究利用 IC 卡的安全特性，將憑證機構發的 Private Key 存入 IC 卡中，在進行 IPv6 之 IPSec 通訊時由 IC 卡讀出，使得互相認證機制更強固，進一步強化 IPv6 互連系統的安全性。

關鍵字：IPv6、IPSec、IKE、AH、PKI、ESP、X.509

1. 研究動機

IC 卡記憶容量大，資料可重複多次寫入或更新，且 IC 卡是屬高科技的產品，一般人能偽造的機會不高，甚至可做到持卡人身分識別、卡片真偽辨識、資料存取控制、內存資料加密、而且成本很低。基於以上幾點，因此我們將利用 IC 卡的這些特性，將 IPSec 認證的 Private Key 寫入 IC 卡中，使互相認證機制更強固，以強化 IPv6 互連系統的安全性。

目前 IPv6 及 IPSec 可以由多種作業環境來實做，但是目前 unix-like 的作業系統支援的標準比 Microsoft Windows 還多，因此我們使用較多人使用的 linux 來作為研究環境，但是 linux 環境下的 IC 卡讀寫，技術上較不普遍，需要進行一些研究測試。而要讓整個系統能完整結合也必須研讀 IETF 相關的 RFC 文件，對於 Linux 中相關的原始碼也必須研究，這些都是我們要克服的問題。

將 IC 卡及 PKI 和 IPv6 的安全機制（IPSec）結合，以提高 IPv6 整體安全性，我們計畫將 IPSec 中用來認證的 Private Key 寫到 IC 卡，目前 RFC 2409（Internet Key Exchange）中有四種身分認證方式的其中一種，經由身分認證確認對方身分正確無誤後，再進行通訊。建立出來的成果就是 IPv6 環境的 IPsec VPN。[2]

2. IPv4 的問題

目前 Internet 已與人們的生活緊密的結合在一起，其中的推手非網際網路通訊協定 （IP）莫屬，但 IP 協定 IPv4（IP version 4）係於 1975 年訂定，已是三十多年前設計的協定，在面對愈來愈複雜、多樣化的網路應用時，已明顯無法滿足要求，特別是在網路通信安全、服務品質保障、服務品質分級、行動通訊及位址數量等方面的限制，勢必將影響未來網際網路的發展。而其他諸如路由器中路由表太大，導致路由器效能不彰，網路組態設定複雜，都是 IPv4 產生的限制及問題

在 IP 數量不足方面，雖然 NAT（Network Address Translation）與 CIDR（Classless InterDomain Routing）等技術，暫時的解決了目前位址資源不足的情況，但長期來看，仍然無法從根本上解決 IP 位址不夠的問題。而且多了一層 NAT 會降低網路傳輸效能，甚至有些 NAT 無法完整保留 IP 表頭的訊息也會某些高層的應用失敗。

3. IPv6 的特性

3.1. IPv6 的歷史[14]

爲了解決前述的 IPv4 的問題並提供了有效的解決方案。1990 年代初期 IETF（Internet Engineering Task Force）開始發展 IPv4 的下一代協定，目的在解決 IP 位址不足的問題，並提供更多的新功能。1974 年 IPng Area 提出創建 IPv6 的建議，也就是 RFC 1752 The Recommendation for the IP Next Generation Protocol。其次 IETF 的 ALE（Address Lifetime Expectation）Working Group 也根據當時的統計資料推斷，IPv4 的位址可能會在 2005 年至 2011 年之間用完。

由於更換成 IPv6 網路，會增加添購設備成本，以致大部分企業尚在觀望中，使得 IPv6 尚未普及，但有一項直得注意的消息是美國國防部於 2003 年宣布未來的網路設備採購必須將支援 IPv6 列入採購規格，而有些美國政府的新計畫如 Esnet 及 DREN 也都將 IPv6 協定列為標準，因此，IPv6 當是未來相當有發展潛

力的領域。

3.2. IPv6 的特點

作為 Ipv4 之後的下一代通訊標準，IPv6 有下列特色：[6] [15]

一、 大量的位址空間： IPv6 使用 128 個位元對網路上的節點定址，定址空間高達 2^{128}，平均地球上每個人可以分到一百萬個IPv6 位址，屆時生活中的各種物品如電視、音響、遊樂器、數位相機、電話、手機、冷氣機、冰箱、微波爐、熱水器、瓦斯爐、計程車、汽車、住家等，都將可能擁有一個IPv6 位址，而成為網際網路上的一員。IPv6 位址空間使用階層式的方式劃分為三層，各層負責授權IP網段給其下層機構，這種管理方式使得交換的路由資訊變得非常精簡，因此會有較佳的路由效率。[8]

二、簡化的表頭格式：IPv6 表頭只有 40 bytes 的固定長度。IPv6 的表頭欄位只有 8 個，而 IPv4 有 12 個。中間路由器需要處理欄位也由 IPv4 的 6 個降成 4 個，因此轉發 IPv6 封包會比 IPv4 更有效率。IPv4 中較少使用到的欄位，被移到擴展表頭（Extension headers），而擴展表頭也可以實現新功能的擴展。IPv6 共移除 6 個 IPv4 的欄位，新增 2 個欄位，重新定義 3 個欄位。[10]

三、內建 IPSec 安全機制：對於身分認證、資料完整性、資料加密的支援，都已成為內建，並已標準化，一定程度上解決了網路安全問題。

四、Flow labeling 保證服務的品質（QoS）：爲解決網路的服務品質問題，IPv6 提供了流標記（flow label），發送端可以將屬於相同資料流，但需要特別處理或有服務品質需求的封包加上標籤（label）。配合 MPLS（Multiple Protocol Label Switch）技術，可作為服務品質控制的依據。IPv6 和服務品質相關的欄位除了 flow label 之外，還有 Traffic Class 欄位，這些都有助於服務品質控制機制的設計。

五、自動的位址配置：IPv6 網路上的主機可以自動取得 IP 不需手動設置。在 IPv4 中，動態主機配置協定（Dynamic Host Configuration Protocol，DHCP）實現了主機 IP 位址及其相關配置的自動設置。IPv6 繼承了 IPv4 自動配置服務，並將其稱爲全狀態自動配置（stateful autoconfiguration）。除了全狀態自動配置，IPv6 還採用了一種被稱爲無狀態自動配置（stateless autoconfiguration）的自動配置服務，由主機根據它的網卡

MAC 位址，自動產生一個 link-local 的 IPv6 位址。

4. IPv6 內建的安全機制-- IPSec

IPSec 提供了一種標準、安全以及具有彈性的機制，可用來爲 IP 及上層協定（如 UDP 和 TCP）提供安全的保證。IPSec 爲了保障 IP 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麼樣的通信（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，以確保不同的實作方案相互之間能具備互通性。如果想增加新的演算法，過程也非常容易，而且不會破壞互通性。因此，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。[1]

4.1. IPSec 架構

IPSec 協定主要包括下列元件：AH （Authentication Header）、ESP（Encapsulation Security Payload）、IKE （Internet Key Exchange）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一來表示：[11]

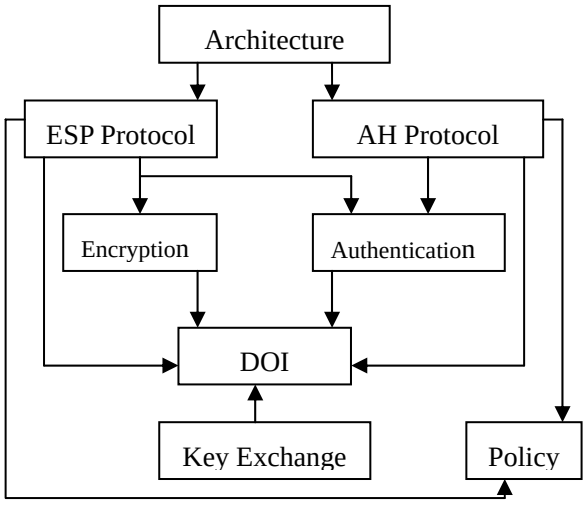


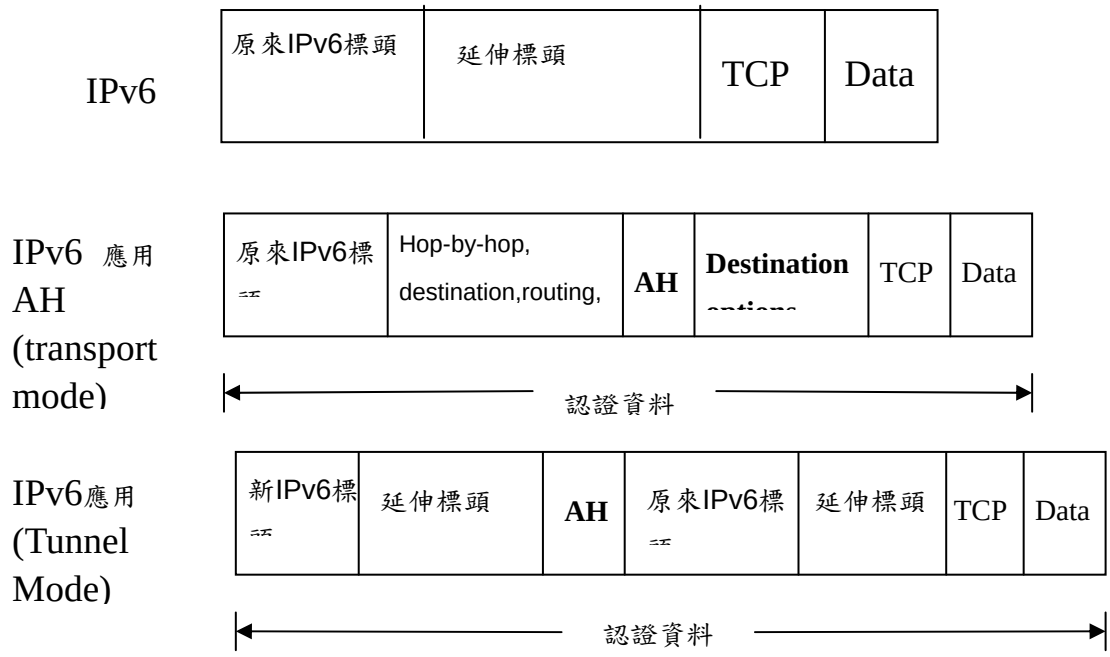
圖1： IPSec體系[9]

IPSec 可使用 AH[13] （Authentication Header）、ESP [12]（Encapsulation Security Payload）這兩個協定來保障安全通信，ESP 可爲 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 可爲 IP 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

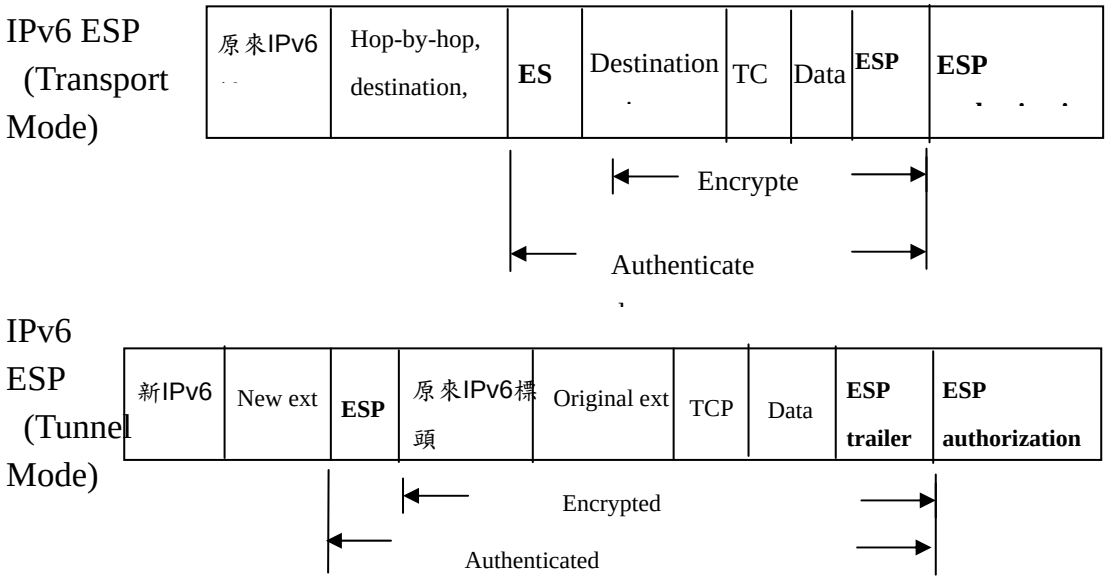
及認證演算法，而 AH 只有認證演算法[7]。IKE （Internet Key Exchange）用來協商溝通雙方，爲 IPSec 產生密鑰。而協商時使用的參數則被歸在一個的文件中，名爲 IPSec DOI（Domain of Interpretation）[5]。目前尚未成爲標準的一個重要元件是“策略”（Policy）。策略是一個非常重要的問題，因爲它決定兩個實體之間是否能夠通信；如果能的話，要採用哪一種轉碼方式（Transform Method）。如果策略定義不當，可能導致雙方通信無法達到要求水準。

4.2. **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（傳送模式）、AH 的 Tunnel Mode（通道模式）、ESP 的 Transport Mode 以及 ESP 的 Tunnel Mode。大部分 IPSec Tunnel Mode 的實作都希望具有機密性，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，它們保護的資料範圍不同，一個是 IP 整個封包，一個是 IP Payload。圖二是 AH 對封包的處理，圖三是 ESP 對封包的處理。



圖二 IPSec AH對IPv6封包之處理



圖三 IPSec AH對IPv6封包之處理

4.3. 、安全聯盟[3] [4]

Security Association（安全聯盟，簡稱 SA）是 IPSec 很重要的基礎。Internet Key Exchange（IKE）即用於動態建立 SA，在 IPSec 中使用 IKE 協商出 SA，並填入 SADB 資料庫中。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（Security Association Database ,SADB），由 SADB 來維護 IPSec 用來保障資料封包安全的資訊。[3]

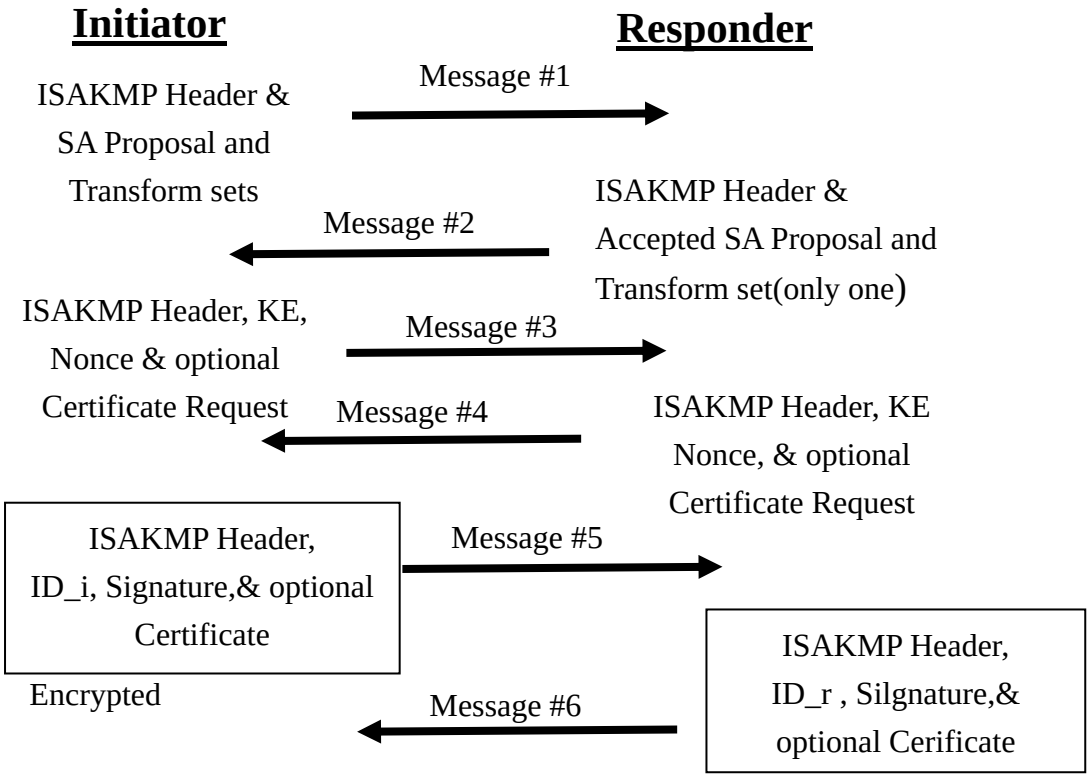
SA 是單向的。因此如果兩個主機（比如 A 和 B）正在通過 ESP 進行安全通信，那麼主機 A 就需要有一個 SA，即 SAA (out)，被用來處理外出的資料封包；但還需要有另一個不同的 SA，即 SAA (in)，用來處理進入的資料封包。主機 A 的 SAA (out)和主機 B 的 SAB (in)將會有相同的加密參數（比如說相同的密鑰）。同樣的，主機 A 的 SAA (in)和主機 B 的 SAB (out)也會共用相同的加密參數。由於 SA 是單向的，所以針對外出和進入處理使用的 SA，都分別需要維護一份單獨的資料表。

此外，每種協定都有一個 SA。因此，如果主機 A 和 B 同時通過 AH 和 ESP 進行安全通信，那麼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。

若安全策略要求爲兩個主機建立多個 SA，以便進行安全通信，那麼這些 SA 的集合便稱爲 SA bundles。

IKE 有兩個協商階段，在第一階段（phase 1），通信雙方間建立了一個已經通過身份認證和安全保護的通道，我們可稱之為 ISAKMP SA。在第二階段（phase 2），就可用第一階段的通道，來爲 IPSec 協商安全服務（SA），這個協商結果，我們可稱之為 IPSec SA。其中和本研究有關之身分認證屬於第一階段，身分不對就停止通信。第二階段和本研究較無關，茲不贅述。

圖四就是以 Main mode 搭配數位憑證建立第一階段 IKE SA 的過程，本研究身分認證的就是這個過程。



圖四 Main Mode with Digital Signature

IPSec 體系中有另一個元件，稱爲安全策略資料庫（Security Policy Database，SPD）。在 IPSec 封包處理過程中，SPD 和 SADB 這兩個資料庫需要一起使用。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性質，定義了在什麼模式下使用什麼協定，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及人工兩種。

5. 結合 IC 卡與 PKI 的 IPv6 安全機制

5.1. 支援 IPv6 的作業系統

目前支援 IPv6 及 IPSec 的作業系統已經很普遍，大致上以 BSD variants（OpenBSD、FreeBSD、NetBSD）系統安裝 KAME 最為完備，linux 在核心 2.5.47 之後的版本也支援 IPv6 及 IPSec，可搭配 ipsec-tools 或 isakampd 安裝使用。如果使用 linux 核心 2.5.47 之前的版本，則可安裝 IABG 的 freeS/wan 或 usagi 提供的程式。Microsoft Windows 對於 IPv6 及 IPSec 的支援則相對上較不完備，以 Windows .net 2003 來說，不但不支援 ESP 加密，也不支援使用 IKE 來協商 SA。本研究是以 linux 2.6 核心搭配 ipsec-tools，作為測試平台。

5.2. PKI 簡介

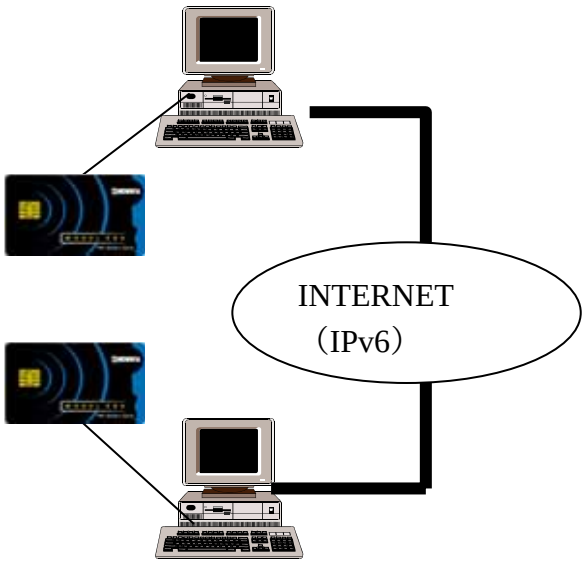
1976 年 Diffie 和 Hellman 在中提出了著名的 D-H 密鑰交換協定，首次提出了公鑰密碼系統。 公鑰密碼系統不需要傳統對稱式秘密交換或分發共用密鑰，而是使用兩把金鑰非對稱式的加密演算法。RSA 是現今使用率最高的公鑰密碼系統。公鑰密碼系統是目前唯一能讓雙方安全分享 Key 的方式。因此，公鑰密碼系統已成為目前電子商務交易的運作基礎。

公開金鑰密碼系統的運作是建立在「通訊雙方能夠正確地取得對方公鑰」的前提之下，所以必須由通訊雙方都信任的公正第三者經一定的程序，驗證個體之身分後簽發憑據，通過憑據把公鑰和身份關聯起來。而簽發憑證的機構稱為憑證機構（ Certification Authority，CA）。也就是說 CA 是除了發給憑證之外，還能證明該公鑰是屬於某個人的公正第三方機構，CA 發出公私鑰對時會先檢驗申請者的身分證明文件（如內政部 CA 要求申請者攜帶身分證親自至櫃檯辦理）。而公開金鑰基礎建設（Public Key Infrastructure， PKI）是運用公開金鑰加密及認證的方法，以確保資料通訊的安全性及確認通訊對方身分的一個機制。因此 CA 是 PKI 架構中一個非常重要的成員。

目前很多軟體都可拿來作為 CA 擔任發放憑證的工作，如 Windows 的 IIS、OpenSSL、OpenCA，本研究以 OpenSSL 為發放憑證程式。安裝 linux 完成，預設就有 OpenSSL，依照手冊中的說明，很容易就可以製造出憑證及私鑰。

5.3.本研究架構

安裝好 linux 之後，接著 compile 2.6 版之後的核心，將 IPv6、IPSec 及加解密演算法相關選項加入核心中，核心編譯成功後，設定好 ipsec.conf 及 racoon.conf 即完成，詳見相關操作說明。通訊的雙方在需要以 IPSec 互通前將 IC 卡插入讀卡機中，由 IPSec 程式讀出，並至 SPD（Security Policy Database）中驗證身分是否正確，只要身分無誤即可進行 IPSec 安全通信。圖五是本研究架構圖。



圖五 本研究架構圖

5.4.研究成果

目前市面上將 Key 放在 IC 卡的 IPSec VPN 產品有 SSH Communications Security Corp，該公司宣稱將 Key 放在 IC 卡中用來做為認證及 auto config VPN 設定，是該產品的一大特性。

但要將 IC 卡中的資料在 linux 環境下讀出，與在 Windows 環境下有所差異，需要選擇可搭配 Linux 的讀卡機及相對應的驅動程式，圖六為讀 IC 卡程式部分原始碼，這個程式把利用 OpenSSL 製作出來放在 IC 卡中的 Private Key 讀出。

```
ezStatus = EzConnectCard(
        ezHandle,0,
```

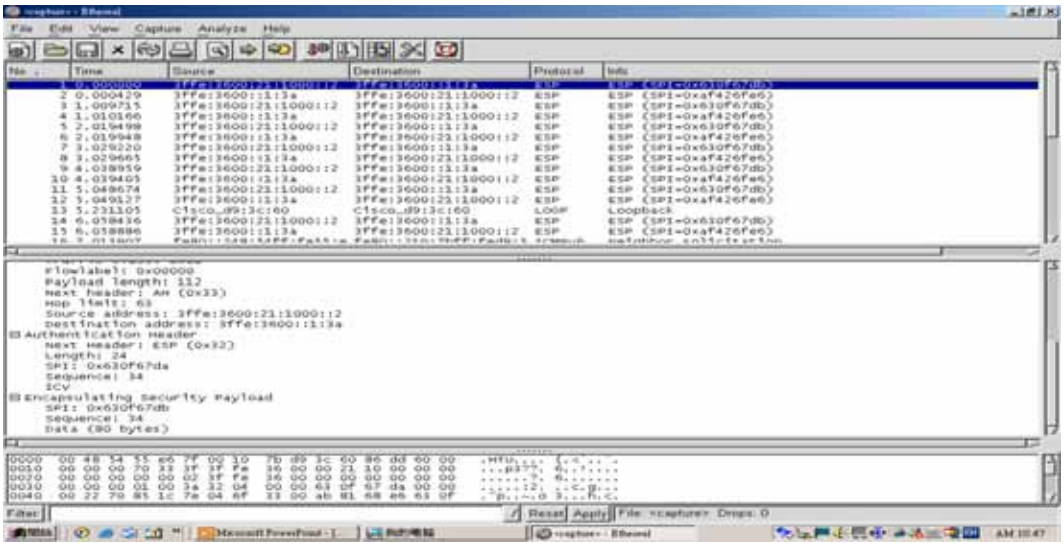
```
                EZSMC_PROTOCOL_T0|EZSMC_PROTOCOL_T1|
                &ulCurrentProtocol,
                &stATR
                );
……
//                              printf("%send",recvbuffer);
                        fp=fopen("ipsecrets","wb");
                        fwrite(recvbuffer,sizeof(char),1000,fp);
```

圖六 讀出IC卡中Private Key的部分原始碼

圖七則是 IPSec 啟動成功，建立了 SA 及 SPD 的畫面。

圖七 IPSec啟動成功建立SA及SPD

從圖八以 Etheareal 擷取的封包，我們可看出 IPSec 確有做封包的處理，AH 及 ESP 的安全機制已經加到 IP 的封包。



圖八 IPSec通訊中Ethereal封包擷取

本研究將 IC 卡結合入 IPv6 中，可把 IC 卡的優點應用在 IPSec 安全通訊環境中，使得 IPv6 的連線更具安全性。將 Key 放在 IC 卡中，主要的優點是當需要 Key 時再由硬體裝置讀出，而 IC 卡是一種低成本設備，並不會增加太多硬體設備花費，可說是目前最安全及最方便的存放憑證及秘鑰的設備。因此本研究的做法可進一步確保 VPN 的整體安全性及更易於認證密鑰管理。

本研究依照 RFC 2409（IKE）的標準，並結合對資訊安全有助益的 IC 卡，使得密鑰管理更完善，再經由 IPv6 內建的安全機制 IPSec，對於資料進一步保護，可使通信系統更具彈性及安全性。

6. 結論

本研究完成由 IC 卡讀出認證的 Private Key，加強網路通訊雙方溝通前的身分認證工作，配合 X.509 的憑證將可做到網路安全上的不可否認性的要求。目前 linux 新的 2.6 核心已將 IPv6 及 IPSec 完全包含在核心中，這也宣示了 IPv6 及 IPSec 安全通信的時代即將來臨，而目前一般提款卡被盜拷的例子，也一再突顯出 IC 卡的高度安全性，因此我們認為 IPv6+IPSec+IC 卡將是未來網路通信安全上的最佳組合，未來還期待更多人投入這個領域的研究。

參考文獻

1. Alcatel Networks Corp.，Understanding the IPSec Protocol Suite ，http://www.alcatel.com/，2000
2. Casey Wilson、Peter Doak ，Creating and Implementing Virtual Private Networks: The All-encompassing Resource for Implementing VPNs， 1999，1st edition, USA The Coriolis Group，372 pages
3. D. Harkins、 D. Carrel，RFC 2409 The Internet Key Exchange (IKE)，IETF，1998
4. D. Maughan， M. Schertler， M. Schneider and J. Turner， RFC 2408 Internet Security Association and Key Management Protocol， RFC 2408，IETF ，1998
5. D. Piper，RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP，，IETF，1998
6. Joseph Davies，Understanding IPv6 ，2002，1st edition，USA，Microsoft Press，544 pages
7. Naganand Doraswamy、 Dan Harkins ，Ipsec: The New Security Standard for the Internet、 Intranets and Virtual Private Networks，2003，2nd edition, USA Prentice Hall PTR，
8. R. Hinden、S. Deering，RFC 2373 IP Version 6 Addressing Architecture ，IETF， 1998
9. R. Thayer、 N. Doraswamy and R. Glenn， RFC 2411 IP Security Document Roadmap，IETF，1998
10. S. Deering、R. Hinden，RFC 2460 Internet Protocol Version 6 (IPv6) Specification，1998
11. S. Kent 、 R. Atkinson，RFC 2401 Security Architecture for the Internet Protocol，IETF，1998
12. S. Kent and R. Atkinson， RFC 2406 IP Encapsulating Security Payload，IETF，1998
13. S. Kent and R. Atkinson，RFC 2402 IP Authentication Header， IETF，1998
14. Silvia Hagen，IPv6 essentials, 2002，1st edition，USA，360 pages
15. 朱永正，新世代 IP 通訊技術與發展現況，中華電信月刊，2004，38 卷第一期，pp.7-20