新一代 SSL 加速器 的實現方式

網路資訊安全已經成為電子商務和網路資訊業發展的一個瓶頸，安全套接層(SSL)協議能較佳地解決安全處理問題，而 SSL 加速器有效地提高了網路安全處理的性能。第一代和第二代 SSL 加速器提高了安全處理性能，但卻不能滿足系統擴展要求，即將推出的第三代 SSL 加速器整合度將更高，並採用新一代匯流排技術實現更高的安全處理性能。

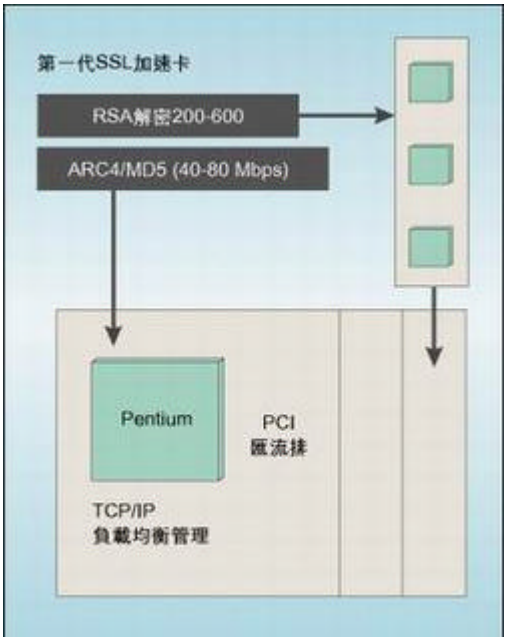
如何實現網際網路的安全性？這個簡單的問題一直困擾著網路的發展。隨著網上信用卡交易的普及與交易量的快速成長，駭客變得更為狡猾，網路互連的安全性已變得越來越重要。

那麼怎樣才能提供最好的安全性呢？利用安全套接層(SSL)協議是個較好的解決方法。

由 Netscape 開發的 SSL 已在網路業得到廣泛的應用，它極大地促進了安全電子商務的發展，使各個公司能安全地開展基於網路的業務。但是，隨著網路設備速度的加快需要大量計算，而速度緩慢的 SSL 正日益顯示出不足之處，它無法以線速度(wire rate)進行安全性處理，而線速度正是當今系統設計工程師所追求的目標。

為了應對這種挑戰，通訊設計工程師們已開發出加速器來加快 SSL 處理。但是這些解決方案仍然不能滿足當今網際網路路設備的要求。

對於大多數通訊業務來說，在系統設計中嵌入 SSL 技術，採用協議加速器而不是僅僅採用密碼加速器 IC 方案才是這個問題的解決方法。在這種想法的推動下，提出了第二代 SSL 加速器與新的 SSL 加速技術，下面將詳細討論並分析這些方案對今後系統設計流程的影響。



SSL 淺析

SSL 是一種對話層協議，位於 TCP 與應用層協議之間。它主要分成兩個複雜階段--握手(handshake)與記錄層處理(record layer processing)。

SSL 握手過程允許客戶機與伺服器系統之間協商修改協議、伺服器識別和共享用於產生數據加密與認証用途的密鑰的保密數據。

握手階段也需要不少功能支援，如安全隨機數的產生、RSA 解密，以及採用一系列散列函數產生主秘(master secret)與密鑰數據。記錄層將位元組數據流處理成記錄塊，並採用密碼套件(cipher suite，一對加密與散列算法)對其進行加密與認証。在記錄層階段採用對稱密碼對用戶數據加密，並採用某種散列算法對數據進行認証，該算法是基於握手階段產生的密鑰。

然而 SSL 性能最大的問題來自產生 SSL 握手的 RSA 不對稱密碼函數。握手協議所要求的計算量非常巨大，可能會消耗系統的所有 CPU 資源，極大地降低系統數據吞吐量。

為了解決這個問題，設計工程師們開發出第一代 SSL 加速器。這些加速器試圖將 SSL 握手(Handshake)部份的負載 RSA 解密移出網路伺服器，讓控制處理器(CPU)來處理餘下的握手函數(用於密鑰創建的散列函數)以及記錄層處理函數(大量的加密與認証)。

一個典型的第一代 SSL 加速器包含一個帶很多 SSL 加速晶片的 PCI 板，每秒最多能處理 200 個解密算法，這比最初的 SSL 產品(不帶加速器)快 30 到 40 倍。

第一代 SSL 加速器

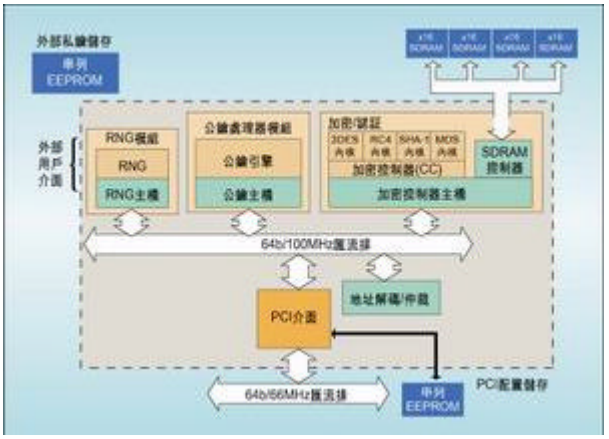
第一代 SSL 加速器每秒能處理 600 個 RSA 解密算法(圖 1)。在全速運行條件下，一個每秒運行 600 個 RSA 解密算法的系統需要約 85Mbps 的加密處理能力，對於 RC4/MD5 密碼套件而言，其負載將佔 1GHz 奔騰 III CPU 處理能力 16%，而 3DES/SHA-1 密碼套件則需要 144%的 CPU 處理能力。

當 RSA 解密功能由 SSL 加速器實現後，CPU 就不會過載，並有足夠能力進行 TCP/IP 處理與記錄層處理。當兩個 SSL 功能單元之間建立平衡後，網路伺服器就能高速發送加密的業務數據，雖然不能接近線速度，但遠遠好於不採用 SSL 加速器的性能。但是，可擴展性是第一代加速器所不能實現的性能。

為了在系統架構中增加更多的 SSL 加速器，設計工程師必須增加更多的伺服器卡。對於設計工程師與運營商來說，顯然是件很困難的事。由於每塊卡的價格要幾千美元，再加上上萬美元的額外伺服器費用，使得這種解決方案的成本迅速攀升。

從性能角度看，由於 CPU 仍要從事大量的加密工作，加速卡數量的增加所提高的效率非常有限。CPU 既要執行越來越多的 TCP/IP 處理，同時又要負責加密計算，因此第一代系統的可擴展性極其有限。

由於上述問題的存在，設計工程師只好又重新尋求新的加速技術，最後他們用單個晶片開發出完整的 SSL 加速產品。



第二代加速器

雖然第一代產品藉由 SSL 加速器處理 RSA 解密功能來提高性能，但系統級的總體性能仍不理想，而採用 IC 形式推出的第二代產品能增加每秒握手次數。

第二代 SSL 加速器設計工程師很快發現需要在握手(Handshake)與加密計算的能力(非同步與同步作業)之間取得均衡，一味地提高每秒內的握手次數只會產生新的瓶頸。隨著密碼套件處理量的增加，CPU 資源很快就會耗盡，也削弱了對 TCP/IP 的處理能力。

例如，即使主處理器採用 1GHz Pentium III 處理器，一個每秒能發送 2,000 次 RSA 握手的純 RSA 解密器也會給主處理器帶來沈重的負載。對於 RC4-MD5 密碼套件來說這些負載將消耗 55%的 CPU 資源，而對於需要大量計算的 3DES-SHA1 密碼套件來說可能需要近 500%的 CPU 資源。

迅速增加握手次數將使瓶頸後移到 CPU，這時，只要記錄層存在大量加密處理就將產生系統阻塞。

為了避免這種瓶頸問題，晶片與系統設計工程師開始尋求用 IC 來實現 SSL 加速。這些通常被稱為網路安全處理器的 IC 會卸載主處理器的握手函數(RSA 解密與密鑰產生)以及記錄層的大量加密與認証函數，使 CPU 能騰出更多的資源來執行封包處理，從而提升系統總體性能。

採用 SSL 加速器 IC 的優勢在於能分擔主機上的 SSL 協議處理，以及提供更多 RSA 解密的能力。為了使這些 IC 能充分發揮系統級性能，所有 SSL 組件必須協同工作。為了給完整的 SSL 協議提供服務，安全處理器晶片上需要整合多個公用組件，包括隨機數產生器、公鑰加密模組和密碼加密/認証模組。

除了服務整個 SSL 協議外，網路安全處理器 IC 必須能快速處理數據的輸入輸出。為了實現這個目的，這些處理器必須優先採用 66MHz/64 位元 PCI 匯流排。為了加快數據的輸入輸出速度，隨機數產生器、公鑰引擎與密碼加密/認証模組一般應鏈接在同一 PCI 匯流排上，這樣在系統設計中能方便地將它們鏈接到其它 PCI 架構。

為了進一步方便整合，製造商還需將安全處理器置於 PCI 板上。因此，製造商需要解決一般 OEM 廠商都會遇到的 I/O 困難，尤其在將這些 IC 置入 PCI 系統架構的時候。

加速器的實現

實現第二代 SSL 加速器 IC 的一個關鍵問題是在系統架構的何處實現。事實上，這些元件可以在網路的 SSL 設備、第 4 層/第 7 層交換機和網路伺服器中實現。

在目前典型的 IP 網路結構中，業務是藉由 L4/L7 智慧負載均衡交換機進入數據中心。輸入的網路客戶機請求將被分配到後端的若干網路伺服器或網路緩衝器中。L7 應用數據在送入網路伺服器之前要做一定的解析。由於 SSL 要加密 L4 以上的所有數據，在數據被完全解密前無法執行對應用層數據的智慧內容交換。

在目前的架構中，SSL 加速功能很可能以單個 PCI 附加卡的形式配置於 SSL 設備和網路伺服器中。交換機將 SSL 業務直接轉移到該設備中並在那裏執行解密，然後設備將未加密的業務數據送回到交換機，這些數據與解密的應用數據進行負載均衡。

緊密整合的下一步是將 SSL 加速器直接整合到 L4/L7 交換機中。要做到這一點，網路安全處理器可以附加在代理卡上(而不是一塊簡單的 PCI 板)，在代理卡上還應黏著運行 SSL 代理程式的控制處理器。這種設備基本上能代替加速設備，可直接集到進交換機埠。

網路安全處理器也可直接配置在網路伺服器中。這種方式對較小型的企業特別有效，因為這些企業通常不會配備大型的伺服器陣列和網路交換機。

在當前架構中，SSL 加速功能很可能以單個 SSL 附加卡的形式配置在網路伺服器中。從發展的角度看，某些情況下的 SSL 加速器配置可以移植到用戶卡，因為加速系統會更直接地整合到總體系統設計中。

本文小結

目前，設計工程師們正在努力開發第三代 SSL 加速器。這種能提供真正千兆位元加密數據流的第三代加速器有望在今年夏季面市。為了實現這一目標，一個均衡系統每秒將至少發送一萬次 RSA 握手，這個目標已經成為加密型全雙工千兆位元乙太網路的非正式標準。要達到如此高的性能，需要在第二代晶片的基礎上對結構作出重大修改。

為了滿足千兆位元傳輸速率的基本性能要求，第三代加速器需要將隨機數產生器、公鑰引擎和加密/認証模組整合在同一晶片上。這些功能模組需要採用高速專用處理內核用於平行運行的密鑰加密運算(AES、MD5、SHA-1、3DES 和 ARC-4)，並採用新一代匯流排技術，如 PCI-X、HyperTransport 或 3GIO。

{註}：以上文章取材自 電子工程專輯
http://www.eettaiwan.com/ART_8800271537_675327_09b46891.HTM