

互聯網規約版本6（IPV6）的保安

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 介紹.....	3
II. 保安考慮.....	5
針對 IPv4 的保安改進.....	5
可能之威脅與其對策.....	6
IPv4 與 IPv6 之常見攻擊.....	7
IPv6 之轉換.....	7

摘要

較新版之互聯網規約版本 6 (IPv6) 規約雖解決了一些在互聯網規約版本 4 (IPv4) 網絡中所發現的保安問題，但並非全部都已解決。舉例而言，在 IPv6 規約中，互聯網規約保安 (IPsec) 是強制的，比舊版之 IPv4 標準更加安全。然而，即使 IPv6 規約擁有彈性，依然會產生新的問題。IPv6 規約建構了一個流動的互聯網規約，但針對這個流動互聯網規約的保安解決方案則尚未開發完成。

此外，IPv6 之動態配置彈性 (如 Stateless Address Auto-Configuration) 如果沒有正確執行，也會成為一個嚴重的保安問題。整體強化的 IPv6 可以在某些特定領域提供更好的保安，但攻擊者仍然可能攻擊規約的一部份。本文將針對 IPv4 在保安上的改進，同時也檢視對 IPv6 的可能威脅。

I. 介紹

目前通行的互聯網規約標準可以追溯到 1970 年代所開發的 IPv4（互聯網規約版本 4）。IPv4 有許多眾所皆知的限制，包括有限的互聯網規約位址空間以及缺乏保安性。IPv4 的互聯網規約位址字段設計是 32 數元，因此可用位址空間很快使用盡。IPv4 所提供的唯一保安功能是保安選項是讓主機以安全方式送出並處理限制參數¹的方法。

基於上述的問題，互聯網工程專責組（Internet Engineering Task Force, IETF）已開始著手進行 IPv6（互聯網規約版本 6）的詳細規格，以便處理這些有關效能、設定的簡易度和網絡管理等的限制議題。IPv6 核心規格是根據好幾個 Request for Comments（RFCs）所制訂，如 RFC 2460²（IPv6 規約），RFC4861³（IPv6 Neighbour Discovery），RFC4862⁴（IPv6 Stateless Address Auto-Configuration），RFC4443⁵（針對 IPv6 之 Internet Control Message Protocol（ICMPv6）），RFC4291⁶（IPv6 Addressing Architecture）以及 RFC4301⁷（Security Architecture for IP or IPsec）。IPv6 也作為下一代的互聯網規約（Next Generation Internet Protocol, IPng）標準。IPv6 與 IPv4 標頭格式（header format）上的不同概述如下：

1. IPv6 標頭格式

¹ <http://www.ietf.org/rfc/rfc0791.txt>

² <http://tools.ietf.org/html/rfc2460>

³ <http://tools.ietf.org/html/rfc4861>

⁴ <http://tools.ietf.org/html/rfc4862>

⁵ <http://tools.ietf.org/html/rfc4443>

⁶ <http://tools.ietf.org/html/rfc4291>

⁷ <http://tools.ietf.org/html/rfc4301>

IPv6 Header

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

2. IPv4 標頭格式

IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

有關 IPv6 規約新的特徵可概述如下：

1. 新的標頭格式
2. 更大的位址空間（128 數元，IPv4 則為 32 數元位址空間）
3. 有效率以及具階層性的定址與路由基礎建設
4. 兼具 stateless 與 stateful 的位址配置
5. 互聯網規約保安
6. 較佳的服務質素（Quality of Service, QoS）支援
7. 有關鄰近節點互動的新規約
8. 可伸展性

強化的 IPv6 在某些地方提供較佳的保安，但亦有一些範圍仍是開放給攻擊者入侵的。

II. 保安考慮

針對 IPv4 的保安改進

大量的互聯網規約位址空間

增加埠掃描 (port scanning) 的難度

開始入侵時，攻擊者通常會先執行埠掃描的偵察技術，以盡可能蒐集受害者網絡的資料。根據估計，在足夠的帶寬⁸下，整個以 IPv4 為基礎的互聯網可以在約十小時左右便掃描完畢，因為 IPv4 位址寬度只有 32 數元。IPv6 則把位址寬度擴充至 128 數元。如此大量位址空間就形成一個有效屏障，阻止攻擊者進行完整埠掃描的企圖。

然而，除了較大互聯網規約位址空間外，用於 IPv6 的埠掃描偵察技術基本上和用於 IPv4 的技術是一樣的。因此，現行用於 IPv4 的最佳作業實務，如過濾邊界路由器 (border routers) 中的內部使用之 IPv6 位址，以及過濾防火牆的非使用服務，應在 IPv6 網絡中繼續使用。

Cryptographically Generated Address (CGA)

在 IPv6 中，將一個公開簽署密碼匙和一個 IPv6 位址連結在一起是可能的。這樣所產生的 IPv6 位址稱為 Cryptographically Generated Address (CGA)⁹。這可為 IPv6 鄰邊路由器 (neighbourhood router) 的探索機制 (discovery mechanism) 提供額外的安全保護，並且允許使用者為特定的 IPv6 位址提供 “proof of ownership” 以證明其擁有權。這是 IPv6 和 IPv4 的主要差別，而將這項功能運用於僅有 32 數元位址空間限制的 IPv4 是不可能的。CGA 提供以下三項主要優點：

1. 使仿冒與竊取 IPv6 位址的攻擊更加困難
2. 允許擁有着利用私人密碼匙替信息簽署
3. 毋需對整個網絡基礎作任何的升級或修改

⁸ <http://www.opte.org/history/>

⁹ <http://www.ietf.org/rfc/rfc3972.txt>

互聯網規約保安 (IPsec)¹⁰

互聯網規約保安，或簡稱 IPsec，為互聯網規約層 (IP layer) 上的傳輸，提供互用的、高質素及以加密為基礎的保安服務。IPsec 的功能在 IPv4 中是選擇性的，但在較新的 IPv6 規約裡，IPsec 已被修改為強制性的功能。IPsec 藉著提供認證、完整性、保密性以及透過 AH (Authentication header) 和 ESP (Encapsulating Security Payload) 兩個規約的使用，對每個 IP 小包的接達控制等來增強原本的互聯網規約。

Neighbour Discovery (ND) 規約取代 ARP 規約

在 IPv4 規約裡，第二層 (L2) 位址並非與第三層 (L3) 位址靜態地連結。因此，在規約沒有作出明顯改動的情況下，IPv4 可在任何第二層媒體之上執行。L2 與 L3 位址的連結是由一個名為 ARP 的規約所建立的。ARP 在區域網絡區段上，建立了 L2 與 L3 位址之間的動態對映。ARP 也有其保安漏洞 (如 ARP 仿冒)。而 IPv6 規約則不需要 ARP。理由是，在 L3 上 IPv6 位址的 interface identifier (ID) 部份是直接取於一個裝置專用的 L2 位址 (MAC 位址)。在 L3 上的 IPv6 位址和它在區域取得的界面 ID 部份會用於整個 IPv6 網絡的所有位址層。因此，與保安議題相關的 ARP 就不再出現於 IPv6 中。由 RFC4861¹¹ 所定義，名為 Neighbour Discovery (ND) 的新規約，將取代 ARP 而用於 IPv6 之上。

可能之威脅與其對策

Neighbour Discovery 與 Stateless Address Auto-Configuration

Neighbour Discovery (ND) 是用來取代 ARP 的。而 Stateless Address Auto-Configuration 則是一個 ICMPv6 裡類似 DHCP 的輕量式功能。它允許一個 IPv6 主機在與 IPv6 網絡作連結時進行自動配置。這兩個都是 IPv6 規約裡有力且具彈性的選項。然而 ND 受到攻擊還是有可能的，這會導致網絡小包流向沒有預期的地方，因而可能受到拒絕服務攻擊的後果。這樣的攻擊同時會允許節點去攔截並選擇性地修改小包而使小包傳到其它節點。IPv6 ND 的保安問題除了可由 IPsec AH 來加以保護外，還可透過 RFC3756¹² 裡包含三種不同信賴模式的 IPv6 Neighbour Discovery (ND) Trust Models and Threats 來解決。

¹⁰ RFC4301 (<http://tools.ietf.org/html/rfc4301>)

¹¹ <http://tools.ietf.org/html/rfc4861>

¹² <http://tools.ietf.org/html/rfc3756>

這三種不同的信賴模式，大致上對應到保安機構內聯網、公開無線接達網絡以及純粹臨機操作的網絡上。

互聯網規約網絡（版本 4 或版本 6）的 Neighbour Discovery 以及路由請求（router solicitation）是使用 ICMP 的。ICMPv4 是一個不屬於 IPv4 的個別規約，而 ICMPv6 則是可以直接在 IPv6 規約上執行的完整規約，因此又會導致保安問題。

在 IPv6 規約之上交換含有重要網絡健康狀況及環境請求的 ICMPv6 信息，對於 IPv6 通訊而言是很重要的。然而，因拒絕服務、傳輸再路由（traffic re-routing）或其它惡意目的所送出的小心偽造的回應信息，會導致 ICMPv6 之信息交換遭到濫用。基於保安上的理由，IPv6 規約建議所有的 ICMP 信息使用 IPsec AH，使其能夠提供完整性、認證以及反轉送（anti-relay）功能。

不使用 ND，而使用預設路由器把重要系統作為靜態鄰邊入口（static neighbour entries），是比較好的做法。這樣可以避免許多典型的 neighbour-discovery 攻擊，但因需要大量的管理工作，造成實際執行上的困難。

IPv4 與 IPv6 之常見攻擊

IPv6 無法解決所有的保安問題。基本上，IPv6 無法避免在對網絡層以上各層之攻擊。IPv6 無法處理的可能攻擊包括：

1. 應用層（Application Layer）攻擊：在應用層（OSI 第 7 層）上所執行的攻擊，如緩衝溢出、電腦病毒與惡性程式碼，網上應用系統攻擊等等。
2. 對認證模組的暴力攻擊與猜測密碼攻擊。
3. 虛假設備（Rogue Device）：未經授權的裝置進入網絡中。裝置可能是一部個人電腦，但也可能是轉接器、路由器、領域名稱系統（DNS）伺服器、DHCP 伺服器或甚至是一個無線接駁點。
4. 拒絕服務：如前所述，拒絕服務攻擊的問題依然存在於 IPv6 裡。
5. 社交攻擊：如濫發電子郵件、仿冒詐騙等。

IPv6 之轉換

轉換工具允許 IPv4 應用程式連結到 IPv6 服務中及 IPv6 應用程式連結到 IPv4 服務中。然而，若沒有周詳地考慮保安問題，攻擊者還是有可能入侵的。

IPv6 版本轉換技術有好幾種，如 6to4（定義於 RFC3056¹³）、Simple Internet Transition（SIT）隧道¹⁴、與 IPv6 上之用戶數據報規約（UDP 如 Teredo¹⁵）。IPv6 的傳輸會經由這些方法進入網絡裡，但是管理者並不意識到使用 IPv6 已經造成網絡漏洞。此外，許多防火牆允許 UDP 的傳輸，讓 IPv6 上的 UDP 在管理者不知情下避開防火牆。攻擊者也可使用 6to4 通道避開入侵偵測系統的偵測。一些防火牆產品只能夠過濾 IPv4 的傳輸，而無法過濾 IPv6 的傳輸。攻擊者會利用這個漏洞，使用 IPv6 的小包進入網絡。

SIT 隧道與隧道路由器（tunnelling router）可以讓 IPv6 在龐大的 IPv4 網絡中單獨進行設置，而且不需要 IPv6 路由器直接地相互連結。這項安排允許入侵者破壞簡單的工作站，並利用他們作為路由器，在沒有連累基礎建設的路由器或防火牆的情況下，直接通行整個子網絡。

在 IPv4 與 IPv6 混合型網絡的主機保安方面，IPv4 與 IPv6 版本之應用程式同樣會遭受攻擊。因此，如果要阻斷傳輸，就必須在任何一個主機控制系統（防火牆、虛擬私有網絡客戶端、入侵偵測系統等等）上，阻斷這兩個互聯網規約版本的傳輸。

¹³ <http://tools.ietf.org/html/rfc3056>

¹⁴ <http://playground.sun.com/ipv6/ipng-transition.html>

¹⁵ <http://www.microsoft.com/technet/network/ipv6/teredo.msp>