

互聯網規約版本6（IPv6）的保安

2011 年 5 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
A. 針對 IPv4 的保安改進	5
B. 潛在的威脅與對策	6
C. IPv4 與 IPv6 之常見攻擊.....	8
D. IPv6 之轉換	9
III. 良好作業模式.....	10

摘要

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，但有些地方可能仍然會被攻擊者利用以作攻擊。本文將針對 IPv6 在保安上的改進，可能的威脅，應注意的保安事項，和部署 IPv6 的良好作業模式。

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讓主機以安全方式送出並處理限制參數¹的保安選項。

因此，互聯網工程專責組（Internet Engineering Task Force, IETF）開始著手進行 IPv6（互聯網規約版本 6）的詳細規格，以解決這些限制以及性能、易於配置和網絡管理等問題。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

IPv6 Header

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

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>

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 規約新的特徵概述如下：

1. 新的標頭格式
2. 更大的位址空間（IPv6 為 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

A. 針對 IPv4 的保安改進

1. 大量的互聯網規約位址空間

增加埠掃描（port scanning）的難度

攻擊者在開始入侵前，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“所有權證”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. 允許擁有者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>

2. 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 IPv6 規約裡則是一項提昇強制性的功能。IPsec 藉著提供真確性、完整性、保密性以及透過 AH (Authentication header) 和 ESP (Encapsulating Security Payload) 兩個規約對每個 IP 小包的接達控制來提昇原本的互聯網規約。

3. 以鄰居發現 (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 L2 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)。IPv6 規約則不需要 ARP，因為 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，加上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 ARP 相關的保安問題就不再存在於 IPv6 中。RFC4861¹¹ 所定義的一個名為鄰居發現 (ND) 的新規約，將取代 ARP 而用於 IPv6 之上。

B. 潛在的威脅與對策

1. IP 位址的構造

IP 位址的構造決定網絡的結構。設計良好的位址構造可減少由 IPv6 新功能所帶來的潛在風險。當設計 IPv6 網絡時，應考慮下列因素。

編號計劃 (numbering plan) 與階層性的定址

編號計劃記錄如何分割其 IPv6 位址的編配。例如，一個機構採用一個 16 子網絡位元 (subnet bit) (即/48) 的地址區塊 (address block) 的話，它可支持最多 65,000 個子網絡。一個好的編號計劃，能在日常保安操作上，簡化接達控制清單 (access control list) 和防火牆規則。它亦更易辨識網站、連結和界面的擁有權。機構應考慮以下列的子網絡方式，小心地計劃並建立一個階層性的網絡。

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

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

- 順序編號子網絡
- VLAN 編號
- IPv4 子網絡編號
- 網絡的所在位置
- 機構內的功能單位(如會計、營運等)

可追蹤的 EUI-64 位址的問題

IEEE EUI-64 位址¹²代表 IPv6 的一種新的網絡界面的定址。網絡界面的 EUI-64 位址，是從網絡界面的物理位址(MAC 位址)演算出來的。通過自動配置，界面的整體 IPv6 位址(global IPv6 address)可以從網絡識別碼(network identifier)和 EUI-64 位址中產生。攻擊者透過 EUI-64 位址，有可能探知遙距電腦的品牌和型號，並藉此找尋攻擊目標。為減低風險，應利用加密算法(例如 CGA)或以 DHCPv6 分配位址的方式，使用不可預測的位址。

2. 未獲授權的 IPv6 客戶端

大多數流行的操作系統和儀器支援 IPv6，因此用戶很容易、甚至不知不覺間啟用了 IPv6。由於 IPv6 加大了功能，以及 IPv6 主機可能擁有數個整體 IPv6 位址的關係，一旦接達控制的設置不當，攻擊者很容易利用這弱點來進行網絡層面的接達。

應考慮下列措施以減低風險：

- 找出啟用了 IPv6 的儀器，並關閉其 IPv6
- 在網絡周邊偵測並封鎖 IPv6 或 IPv6 隧道的通訊
- 在機構的保安計劃內加入 IPv6 使用政策

3. 鄰居發現與不可設定狀況的位址自動設定

鄰居發現 (ND) 是用來取代 ARP 的。而不可設定狀況的位址自動設定 (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 規約裡有力且靈活的選項。然而鄰居發現仍然可能受到攻擊，導致網絡小包流向意想不到的地方，拒絕服務攻擊就是其中一種可能的後果。這種攻擊亦可能被用來攔截，甚至修改傳到其它節點的小包。這保安問題除了可由 IPSec AH 來加以保護外，RFC3756¹³ (IPv6 ND Trust Models and Threats) 還預計了 IPv6 鄰居發現的安全機制可運行在那些網絡上。這三種不同信賴模式，大致可對應為保安機構內聯網、公開無線接達網絡、和純粹臨機操作的網絡。此外，SEcure Neighbor Discovery (SEND) 規約亦提供另一以加密方式來保護鄰居發現的機制。

¹² EUI為 Extended Unique Identifier 的首字母縮略字。例如，“3BA7:94FF:FE07: CBD0”便是一個以冒號十六進位法進行標記的EUI-64識別代號。

¹³ <http://tools.ietf.org/html/rfc3756>

互聯網規約網絡（版本 4 或版本 6）的鄰居發現以及路由請求（router solicitation）是使用 ICMP 的。ICMPv4 是一個獨立於 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，因此也會導致保安問題。

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精心偽造的回應信息，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。

不使用鄰居發現，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鄰居發現攻擊。但這樣做，需要一定的管理工作。

4. 雙操作

機構不可能在一夜之間將其所有網絡轉換為 IPv6。在逐步設置 IPv6 的同時，亦要維持 IPv4，以支援舊有客戶端和服務。一個雙規約的環境，會令操作和保安變得更加複雜。無論如何，機構必須維持現有針對 IPv4 的措施，並確保同等程度的措施也應用於 IPv6 上。機構在執行保安政策時，須確保針對 IPv4 和 IPv6 的政策(包括防火牆和小包過濾方法)為一致。操作期間，管理者應意識到兩種規約的相關威脅和漏洞，並採取適當措施以減低風險。

C. 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、甚至是一個無線接駁點。
4. 拒絕服務：拒絕服務攻擊的問題依然存在於 IPv6 裡。
5. 採用社交網絡的攻擊：諸如濫發電子郵件、仿冒詐騙等技術。

D. IPv6 之轉換

轉換工具允許 IPv4 應用程式連結到 IPv6 服務，以及 IPv6 應用程式連結到 IPv4 服務。然而，若沒有周詳的計劃應對保安問題，攻擊者會利用保安漏洞入侵網絡的。

IPv6 版本轉換技術有好幾種，如 6to4（定義於 RFC3056¹⁴）、簡單互聯網轉換（SIT）隧道¹⁵、與 IPv6 上之用戶數據報規約（UDP 如 Teredo¹⁶）。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 通道避開入侵偵測或防禦系統的偵測。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）容許在眾多 IPv4 網絡中單獨設置 IPv6，而無需 IPv6 路由器直接相互連結。這特性令入侵者可以破壞簡單的工作站，從而利用它們作為路由器，在無需破解作為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。要檢查包裹在隧道內的傳輸，應部署可理解該等隧道傳輸的裝置。此外，應在隧道的出入口執行保安政策。

在 IPv4 與 IPv6 混合型網絡的主機保安方面，需注意主機應用程式同樣可能遭受來自於 IPv4 與 IPv6 網絡的攻擊。因此，如果要阻斷傳輸，就必須一併阻斷這兩個互聯網規約版本在任何主機控制系統（防火牆、虛擬私有網絡客戶端、入侵偵測系統等等）上的傳輸。應該監察 IPv6 網絡的傳輸，審計網絡上的路由請求和鄰居發現，以偵測插入到網絡內的虛假路由器和未經授權設備。

¹⁴ <http://tools.ietf.org/html/rfc3056>

¹⁵ <http://playground.sun.com/ipv6/ipng-transition.html>

¹⁶ <http://technet.microsoft.com/en-us/network/cc917486.aspx>

III. 良好作業模式

下面是一些建設和維護安全的 IPv6 網絡的良好作業模式，以供參考：

- 為關鍵系統使用標準，非顯而易見的靜態位址；
- 確保 IPv6 網絡有足夠的過濾能力；
- 在邊界路由器過濾器內部使用的 IPv6 位址；
- 在只限 IPv4 的網絡上，阻擋所有的 IPv6 流量；
- 在防火牆過濾不必要的服務；
- 制定一個細緻的 ICMPv6 過濾策略並過濾所有不必要的 ICMP 信息類型；
- 維護主機和应用程序的安全，為 IPv4 和 IPv6 使用一致的安全性原則；
- 使用 IPsec 來認證和為資產提供保密；
- 記錄 last-hop traceback 當中的程序；和
- 密切注意過濾機制的保安。