BGP 路由安全之威脅與防護

林書呈
財團法人國家實驗研究院國家高速網路與計算中心
daniellin@narlabs.org.tw

摘要

全球的網際網路(Internet)由不同的自治系統（Autonomous System）所組成，利用邊界閘道協定(Border Gateway Protocol, BGP)決定自治系統之間的最佳路徑，達成彼此互連。 BGP 協定的設計採用信任制，自治系統若是配置錯誤或是惡意散布錯誤的路由資訊，由於協定設計上並無檢查機制，造成路由安全威脅事件層出不窮，也影響全球許多網際網路服務提供者的網路服務。

本文將簡介全球自治系統間採用邊界閘道協定交換路由資訊的運作方式，再來探討此協定目前可能引起的路由安全威脅與近期發生之網路異常事件。接著我們將研究國際網際網路組織目前針對路由安全問題提出的防護建議，並將適當的安全防護機制，實作於我們維運的學研網路骨幹上，期能強化骨幹網路的路由安全防護，提昇網路服務的穩定性。

關鍵詞：路由安全、資源公鑰基礎建設、路由安全規範計畫

Abstract

The global Internet network consists of different autonomous systems (Autonomous System), which use the Border Gateway Protocol (BGP) to determine the best path between them. The BGP protocol trusts the routing information announced from peers. If the autonomous system is misconfigured or maliciously announces the wrong routing information, there is no check mechanism to avoid. This may causes many routing security threats and affects the network connectivity of many Internet Service Providers.

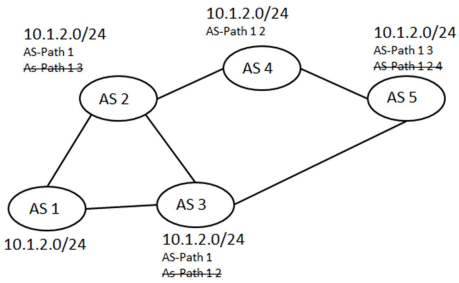
This article will introduce the operation of BGP protocol between autonomous systems. Then we will explore the routing security threats and discuss the network outages caused by route leak or BGP hijack recently. Next, we will study the recommend actions of the international Internet organization for routing security issues, and implement the appropriate security protection mechanism on our research and education network backbone to strengthen the routing security. Hope those actions for routing security will increase the stability of network services.

Keywords: Routing Security、RPKI、MANRS

1. BGP 路由協定

網際網路是全世界最大的電腦網路，由政府、學校、研究單位、民間企業等大小網路相互連結而成。全球的網路管理單位必須向網際網路號碼分配局(Internet Assigned Numbers Authority, IANA)申請專屬的 IP 網路位址及自治系統號碼 Autonomous System Number, ASN)，利用邊界閘道協定(BGP)與其他自治系統交換 IP 網路位址資訊，與全世界的網路彼此連結。BGP 由由網際網路工程小組(The Internet Engineering Task Force, IETF)所制定，是目前自治系統交換路由資訊的標準協定。

BGP 的路由傳播方式如圖一所示，多個自治系統間透過 BGP 協定建立彼此連結關係，並利用 BGP 路由更新交換路由資訊，在路由資訊的欄位上，會帶入自治系統號碼與其他重要的路徑選擇屬性，供最佳路徑判斷使用，如果被選為最佳路徑，就會將該筆路由資訊紀錄在路由表中，並傳播到下一個自治系統，如此傳播下去，所有相連的自治系統都會獲得各自所屬網路的路由資料，達到全網互連之連通性。



圖一： BGP 協定路由傳播示意圖

例如自治系統 AS1宣告10.1.2.0/24的網段，會向有互連關係的自治系統 AS2與 AS3發送， 自治系統 AS2在 AS1與 AS3學到同一筆10.1.2.0/24的路由時，會算出來自 AS1的路由路徑較佳，會放進路由表，依此傳播方式讓整個網際網路的自治系統都可以學到前往10.1.2.0/24的路徑。

2. BGP 路由安全之威脅

BGP 協定自1989創立至今運行至今已30年，在路由功能的設計上相當可靠穩健，仍是自治系統間進行路由交換的主要協定，但是在路由安全的設計上，存在著非常明顯的設計缺陷與安全漏洞。依照 BGP 協定的規範，不同自治系統間進行路由交換時，只能向外宣告本身所擁有的 IP 位址前綴，然而 BGP 協定的設計採取信任制，缺乏一個安全可信的路由認證機制，針對互連自治系統所宣告的任何路由，預設都是默認接受的，無法對收到的路由訊息進行真實性與完整性的驗證，假使一個自治系統對外宣告不屬於自己的 IP 位址前綴，也會被互連的自治系統接受並傳播，這類錯誤的路由傳播也造成許多網路障礙或網路安全的問題發生。

BGP 協定運行於自治系統間，網路上的任一

自治系統都可利用 BGP 協定影響其他自治系統的路由政策，若自治系統的路由安全未妥善掌控，就可能像蝴蝶效應一樣，對整體的網路造成重大的影響。近年來針對路由安全的威脅層出不窮，像是 BGP 挾持與 BGP 路由洩漏的事件，多是利用 BGP 的設計缺陷而來，接著我們介紹幾個最近發生的路由安全威脅事件。

2.1 BGP 挾持(BGP Hijack)

BGP 挾持指的是一個自治系統對外宣告了一個不屬於自己的 IP 位址前綴，可能是其他自治系統所擁有或是尚未配發的網路位址，將直接造成流量挾持的狀況發生。

在2018年4月，駭客集團利用 BGP 協定的漏洞，對外宣告 Amazon DNS 的 IP 位址前綴給互連 ISP[1]，互連 ISP 也將這筆錯誤的路由宣告向外廣播，挾持了大約1300個 IP 位址。駭客集團因挾持 Amazon DNS 網段，將 MyEtherWalletclo 的流量引導至位在俄羅斯的假網站，竊取了用戶的隱私訊息，藉機盜走15萬美金的乙太幣。

在2019年5月，台灣網路資訊中心(TWNIC)營運的公共 DNS 服務 Quad101，封包被導向巴西的網路業者[2]，造成服務影響約 5分鐘。根據事後的調查資料發現，巴西的網路業者當時對外宣告了不屬於他們所有的101.101.101.0/24網段，這筆路由宣告也利用 BGP 協定對外廣播，造成部份連往 Quad101進行 DNS 查詢的封包被導到巴西然後中斷，影響公共 DNS 的服務，巴西的 ISP 在收到通知後也立即修正錯誤，並未讓問題擴大。

2.2 BGP 路由洩露(BGP Route Leak)

BGP 路由洩漏指的自治系統間路由的傳播，超出了原先預期的範圍，違反傳送方或接收方預期的路由政策，造成部份網路流量被轉送到非預期的路徑，可能導致流量被監聽、流量過載或網路黑洞等問題。

BGP 路由洩露所傳播的路由是合法宣告的，只是違反自治系統間的路由策略，這類的問題大多來自錯誤的設定。在2018年11月，中華電信 HiNet 出現部份連接國外壅塞的問題[3]，影響客戶網路連線約30分鐘，經事後調查障礙原因，發現當時中華電信的互連單位台灣智慧光網有進行路由調整，誤將 Internet 的路由廣播給中華電信 HiNet，而 HiNet 也將路由轉發給客戶，造成客戶連往 Internet 的流量被轉向到台灣智慧光網的骨幹，由於台灣智慧光網的骨幹頻寬較小，流量過大造成網路壅塞或網路失聯。

在2019年6月，也發生 BGP 路由洩露將歐洲行動流量流經中國電信的事件[4]。瑞士資料中心代管業者 Safe Host 所管理的自治系統號碼 AS21217，誤將歐洲行動業者的7萬多筆路由，發送給在德國與 Safe Host 互連的中國電信 AS4134，中國電信也將這類錯誤的路由對外廣播，造成許多連往歐洲行動業者的網路流量，都先繞經中國電信的骨幹，再連往瑞士的 Safe Host，由於偏離了原本的最短路徑，使得行動網路的流量出現擁塞或遺失的情況，影響網路服務達2小時。在2019年7月，全球最大的內容傳遞服務商 Cloudflare 也因為美國電信公司 Verizon 的 BGP 路由宣告錯誤[5]，將 Cloudflare 代管的網站流量錯誤導向美國賓州某家小公司，導致這些大型知名網站的服務中斷達2個小時。

這些 BGP 路由洩露的意外也說明了路由安全的重要性，不論網路規模的大小，一個小自治系統的設定錯誤，可能就會對全球網路連線帶來重大的影響，也提醒我們對於互連的自治系統不可完全信任，必須有良善的路由安全管理機制來保護網路的穩定性。

3. BGP 路由安全之防護

根據網路組織針對路由系統的統計資料[6]，光是2018年，全球就有超過12,600次的 BGP 路由洩露或 BGP 挾持的事件發生，至少有2,700個以上的自治系統被路由安全事件影響網路連線，造成資料洩漏、網路連線中斷、數據被盜、收入減損等影響，國際網際網路組織針對路由安全問題，提出多個防護與強化的建議，以下將簡介各種 BGP 路由安全的防護機制。

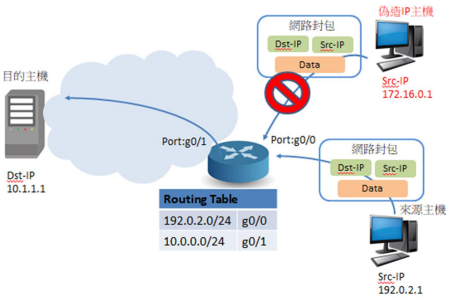
3.1 單播轉向路徑轉發(unicast Reverse Path Forwarding, uRPF)

當路由器接收網路封包時， 正常的處理程序會是找出封包的目的地 IP 位址，比對路由表後找出到目的地 IP 的最佳路徑，再進行封包轉送，由於封包轉送的行為不會檢查來源 IP 位址，給了網路攻擊者一個可乘之機，以 NTP 放大攻擊為例，攻擊者會操縱許多殭屍電腦，送出許多偽造特定來源 IP 位址的封包 ，向 NTP 伺服器提出查詢，由於正常封包轉送不會檢查來源 IP 位址，因此這些封包都會轉送到 NTP 伺服器。 當 NTP 伺服器在收到查詢封包時，會將查詢結果回應給偽造的來源 IP 位址，大量的 NTP 回應封包就會產生分散式阻斷攻擊的效果(DDoS attack)，讓偽造的來源 IP 位址對外網路頻寬壅塞，產生癱瘓網路服務的效果。

為解決這樣的問題，網際網路工程小組(IETF)制定了 BCP38[7]的網路工具，使用單播轉向路徑轉發(Unicast Reverse Path Forwarding, uRPF)的技術，來防堵偽造來源 IP 位址的網路攻擊行為，當路由器的網路接口啟用 uRPF 功能後，在 收到網路封包時，就先針對網路封包的來源 IP 位址進行合法性檢查，檢查通過的封包，才會依照正常處理步驟找出封包的目的地 IP 位址進行最佳路徑找尋與

轉發，若來源 IP 位址合法性檢查失敗，封包就會被丟棄。

uRPF 對於來源 IP 位址合法性檢查的類型分為嚴格型(Strict mode)與鬆散型(Loose mode)。若將接口設定為嚴格型，當網路封包進行來源 IP 位址合法性檢查時，會檢查該來源 IP 位址 是否存在路由表中，並確認網路封包送入的接口與路由表中的出接口一致，才會視為合法封包，否則將丟棄該封包；若是將接口設定為鬆散型，當網路封包進行來源 IP 位址合法性檢查時，僅確認該來源 IP 位址 是否存在路由表中，不再確認網路封包送入的接口是否與路由表匹配，這可使 uRPF 可有效阻止網路攻擊，又可避免錯誤攔截合法網路封包。



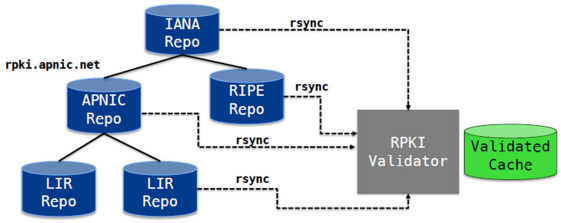
圖二：uRPF 封包來源 IP 檢查示意圖

以上圖二為例，當收到網路封包時，路由器會先找出封包的目的 IP 位址10.0.0.1，對照路由器本身的路由表資訊，將封包轉發到 g0/1接口，當g0/1接口設定 uRPF 嚴格型時，路由器會先找出封包的來源 IP 位址192.0.2.1做合法性檢查，比對此IP 是否存在路由表中，並確認收到網路封包的接口 g0/0是否與路由表中192.0.2.0/24網段的出接口匹配，通過合法性檢查後再找出目的 IP 位址10.0.0.1進行封包轉發的行為，若是有偽造 IP 的主機送出網路封包，由於來源 IP 位址172.16.0.1合法性檢查不會通過，封包就會被丟棄。利用 uRPF 功能的啟用，可有效阻絕偽造來源 IP 位址的網路攻擊行為，確保路由的安全性。

3.2 資源公鑰基礎建設(Resource Public Key Infrastructure, RPKI)

由於 BGP 協定並無檢查路由來源宣告正確性的能力，導致 BGP 挾持的事件層出不窮，嚴重影響網際網路的穩定性，為解決這樣的狀況，RPKI 的技術應運而生[8]。RPKI 的中文全名為「資源公鑰基礎建設」，利用公鑰基礎建設(Public Key Infrastructure, PKI)的框架對 IP 位址所有權進行認證，讓 IP 位址的傳遞能獲得更高的安全性。RPKI 使用 RFC3779定義的 X.509授權憑證格式，將 IP 位址以及自治系統號碼的組合進行簽署，在配發 IP 位址與自治系統號碼時，同時會簽署一張資源憑證給該單位，確認這些資源的所有權。

RPKI 利用路由起源授權(Route Origin Authorization, ROA)的格式，將 IP 位址前綴以及 ASN 進行連結，資源持有單位如 ISP 可利用註冊單位簽署過的 IP 位址終端憑證以及 ASN 終端憑證進行 ROA 的建立，讓 IP 位址前綴與 ASN 的關係連結起來。當 ROA 被建立之後，註冊管理機構就會將一筆一筆的 ROA 紀錄儲存在當地的資料庫中，供網路路由設備連結使用。ROA 紀錄儲存在多個分散式資料庫， RPKI Validator 利用 rsync 週期性的同步這些加密 ROA 紀錄，並儲存一份本地驗證的快取，RPKI Validator 資料同步架構如下圖三所示。



圖三：RPKI Validator 資料同步架構

(Source: https://www.slideshare.net/apnic/peering-asia-20-rpki-for-peering)

當路由器與 RPKI Validator 完成連結設定後，就可以同步本地驗證的快取，作為路由表中 IP 位址前綴來源有效性驗證使用，每一筆 IP 位址前綴比對來源宣告後有以下三種結果：

- 有效(Valid)：代表該筆 IP 位址包含在一個 ROA 元件中，且自治系統號碼一致，是來源合法的 IP 位址宣告。
- 無效(Invalid)：代表該筆 IP 位址包含在一個 ROA 元件中，且自治系統號碼不一致，表示該筆 IP 位址的來源位址是沒有獲得授權的，或者是該筆 IP 位址宣告的前綴長度超過 ROA 中設定的最大長度。
- 未知(Not found/Unknown)：代表該筆 IP 位置並未包含於現有的 ROA 紀錄當中，由於無 ROA 紀錄可供比對，無法確定其來源宣告的合法性。

當路由器啟用 RPKI 的功能之後，路由表中的每一筆 IP 位址紀錄都多了來源宣告驗證的屬性，提供 BGP 協定驗證來源宣告的合法性的能力，有效遏止 BGP 挾持的事件發生。

3.3 路由安全規範計畫(Mutually Agreed Norms for Routing Security, MANRS)

由於 BGP 本身的設計缺陷，造成 BGP 路由洩露與 BGP 挾持的問題日益嚴重，路由安全的議題成為未來全球網路穩定的重要關鍵。為了讓全球的自治系統有一套規範可以遵循，由國際網際網路協會(Internet Society, ISOC)推動一項相互協商的路由安全規範計畫[9](Mutually Agreed Norms for Routing Security, MANRS)，希望集結全球網路商的營運經驗與知識，提供一套路由管理的參考準則，強化網路系統的安全性，減少常見的路由安全威脅。

ISOC 成立於1992年，是一個非政府、非營利的國際組織，負責推動網際網路全球化，加快網路互連技術、提高網際網路普及率等重要工作。

在全球路由安全強化的工作上，ISOC 藉由 MANRS 計畫，提供網路交換中心與網路營運單位一個基本規範來提高網際網路的安全性與可靠性，規範的四個操作步驟如下：

1. 過濾(Filtering)：避免傳播錯誤的路由資訊，藉由與互連自治系統間建立良好的路由過濾策略與 AS 路徑檢查機制，確保路由宣告與路由接收的正確性，防止散布錯誤的路由訊息。
2. 反假冒(Anti-Spoofing) ：確認來源 IP 位址的正確性，藉由存取控制清單的設定以及來源 IP 位址檢查的驗證，防堵假冒 IP 位址的網路流量，大幅降低分散式阻斷攻擊(DDoS attack)的傳播與影響。
3. 協調(Coordination)：暢通全球網路營運單位之間的溝通，藉由即時更新與維護自治系統相關的公開聯絡資訊以及路由資料庫的持續維護，讓網路發生障礙時可以有效率的聯絡，強化全球網路營運單位之間的連結與協調。
4. 全球驗證(Global Validation)：強化全球路由來源宣告驗證之能力，藉由 RPKI 的推動及路由資料的維護與發布，全球網路營運單位可以驗證路由來源宣告，限縮路由挾持事件造成的網路影響。

MANRS 利用上述四個操作步驟，提供一份網路安全強化的最佳參考準則，有效解決錯誤路由宣告以及假冒來源 IP 位址的網路攻擊問題，降低路由異常狀況對網路造成的衝擊； 在協調與驗證兩個部份，則可強化與全球網路營運商之間的連結關係，讓網路異常問題可以更有效率的被解決，降低未來再發生的可能性。截至2019年7月，全球已有包含 Google、Microsoft 等191個網路營運單位以及32個網路交換中心加入此計畫，希望能透過更多自治系統的參與，讓路由安全的問題獲得改善與控制。

4. TWAREN 骨幹路由安全之實作

台灣高品質學術研究網路(TaiWan Advanced Research and Education Network, TWAREN)[10]是為學術研究而設的專用網路，服務對象包含國內各大專院校、政府機關及研究單位等，由國家高速網路與計算中心負責網路維運管理。作為台灣的學術研究網路的維運單位，我們向台灣網路註冊管理機構 TWNIC 申請一個自治系統號碼 AS7539，用來與全球學術研究網路單位進行 BGP 路由互連，也向 TWNIC 申請 IPv4位址與 IPv6位址作為對外提供連線服務使用，為了強化 TWAREN 網路骨幹的路由安全，我們在骨幹設備上實作了 RPKI 的技術，並建立適當的路由過濾策略來確保 BGP 路由安全。

4.1 路由起源授權驗證

台灣網路資訊中心在2018年10月將 RPKI 服務系統(https://myrpki.twnic.tw)[11]正式上線，網站提供 IP 持有單位檢視其資源憑證與新增、修改、刪除路由起源授權元件的功能。本中心在申請帳號之後，也隨即完成 ROA 紀錄之建立與設定，ROA 資料在建立完成後，就會儲存在 TWNIC 的資料庫，並以 rsync 技術定期同步各註冊管理機構建立的 RPKI Validator 伺服器上。

在 ROA 建立完成後，可到台灣網路資訊中心提供的 RPKI Validator 的網站[12]進行查詢，確認 ROA 是否已同步到 Validator 上。以本中心目前對外宣告的 IP 位址前綴211.73.64.0/19為例，在 RPKI Validator 網站的查詢結果如下圖四，狀態為 VALID 代表這筆路由紀錄經 RPKI 系統比對來源宣告驗證的結果是合法的，若有其他惡意網路攻擊或錯誤設定的自治系統宣告本中心的 IP 位址前綴，該筆路由紀錄的狀態將會呈現 INVALID，即可利用 BGP 的來源宣告驗證屬性將其過濾。

圖四：RPKI Validator 來源宣告比對查詢

在網路設備的設定上，我們也將骨幹路由器啟用 RPKI 的設定，並與台灣網路資訊中心提供的 RPKI Validator 建立連結關係，從 RPKI Validator 中獲得 ROA 元件的快取資料，設定完成之後的狀態如下圖五，可看到目前我們已從 TWNIC RPKI Validator 中同步到73,422筆 IPv4 ROA 紀錄以及 13,168筆 IPv6 ROA 紀錄到網路路由設備來，可供比對 IP 位址前綴來源使用。當我們在查詢 IP 位址的路由時，設備會比對 ROA 紀錄並將來源宣告驗證屬性新增到路由資訊中，讓 BGP 協定具備驗證來源宣告合法性的能力，強化骨幹路由安全。

```
RP/0/RP0/CPU0:TWAREN-TN-ASR9912-01#show bgp rpki summary
Fri Jul 19 22:12:09.327 cst

RPKI cache-servers configured: 1
RPKI global knobs
  Origin-AS validation is ENABLED globally
  Origin-AS validity WILL NOT affect bestpath selection globally
  Origin-AS validity signaling towards iBGP is DISABLED globally
RPKI database
  Total IPv4 net/path: 73422/78175
  Total IPv6 net/path: 13168/14341
```

圖五：RPKI 設定完成之狀態

4.2 路由過濾策略

在路由過濾策略部份，為了確保路由宣告與路由接收的正確性，我們參考 MANRS 提供的路由安全強化參考準則與長期維運骨幹網路的經驗，在運行 BGP 協定與外部互連的 TWAREN 骨幹設備上，建立了以下路由過濾策略設定：

1. 設定接收路由筆數上限：在與互連單位建立 BGP 連結關係後，會確認對方宣告路由筆數之範圍，在加上合力的路由變化空間後，設定接收路由筆數上限，以避免互連單位 BGP 路由洩

露造成流量外溢。

2. 過濾不該於網路中流通的 Bogon[13]參考清單：Bogon 清單指的是不應該存在路由表當中的 IP 位址前綴，包含規範於 RFC1918的私有 IP 位址前綴、規範於 RFC5735、RFC6598中的特殊保留 IP 位址前綴以及尚未分配的 IP 位址前綴，這份清單不應該被任何自治系統宣告，在接收互連單位路由資訊時，需先過濾 Bogon 清單內的 IP 位址前綴。
3. 設定 uRPF 於互連接口：在與互連單位連接的界面上，啟用 uRPF 設定，對封包來源 IP 位址進行驗證，舒緩偽造來源地址攻擊的事件造成的影響。
4. 設定 RPKI 路由來源宣告驗證：在與互連單位建立 BGP 連結關係的骨幹路由器上，啟用 RPKI 路由來源宣告驗證的功能，將路由比對結果為無效(Invalid)的捨棄，調降這類路由的優先等級，避免 BGP 挾持的事件影響網路連線。

5. 結論

全球網際網路透過 BGP 協定彼此連結在一起，路由安全的重要性日益增加，如何為自己的網路環境建立良好的防護機制，減少外部問題造成網路異常問題成為一項重要課題，本研究探索目前常見路由安全事件發生的原因，並針對各種安全威脅尋找建議之防護準則，資料彙整如下表一，可供自治系統網路管理者參考採用。

	路由安全威脅	建議防護方式
1	偽造來源 IP 位址攻擊	啟用 uRPF 進行基本防護，並參照 MANRS 防堵假冒來源 IP 位址之事件
2	BGP 挾持	啟用 RPKI 驗證路由來源宣告
3	BGP 路由洩露	設定接收路由筆數上限，並參照 MANRS 防護準則內容，建立適當的路由過濾策略，減少 BGP 路由洩露發生

表一：常見路由安全威脅及其防護建議

TWAREN 提供台灣學術界先進的網路技術研究平台，非常適合新技術的導入，本次將 RPKI 技術實作於 TWAREN 骨幹上，就是希望能夠實際驗證 RPKI 修補現行 BGP 協定無法進行來源宣告驗證的弱點，我們也參照 MANRS 提出的網路安全強化參考準則，調整我們與互連網路之間的路由安全管控策略，希望能讓我們的網路骨幹更加安全與穩定，後續我們也希望加入 MANRS 計畫，與全球的網路營運單位建立更好的連結關係。

由最近發生的一些網路安全威脅事件，我們發現不論自治系統規模大小，若路由安全沒有良好的管理，一個微小的錯誤設定，都可能大範圍的影響網路連線服務，身為全球網際網路中的一個自治系統網路管理者，對於 BGP 路由安全之防護，必須投入更多的心力，才能維護良好穩定的網路環境。

誌謝

感謝台灣網路資訊中心(TWNIC)積極推廣 RPKI 技術，除建立服務系統協助驗證路由來源宣告，也舉辦多場說明會與教育訓練協助國內各級網路營運商設定及啟用 RPKI。

參考文獻

[1]Amazon DNS 53 BGP 挾持事件
https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/
[2]台灣網路資訊中心公共 DNS 挾持事件
https://www.manrs.org/2019/05/public-dns-in-taiwan-the-latest-victim-to-bgp-hijack/
[3]中華電信 HiNet BGP 路由洩露事件
https://www.cht.com.tw/zh-tw/home/cht/messages/2018/msg-181121-205000
[4]BGP 路由洩露造成流量外溢
https://www.ithome.com.tw/news/131157
[5]Cloudflare 代管網站 BGP 路由洩露事件
https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/
[6]ISOC 網路攻擊統計
https://www.internetsociety.org/blog/2019/02/routing-security-getting-better-but-no-reason-to-rest/
[7]IETF BCP38
https://tools.ietf.org/html/bcp38
[8] 林書呈, 利用 RPKI 強化路由安全之實作, 第十八屆離島資訊技術與應用研討會, 2019年5月
[9] MANRS 計畫網站
https://www.manrs.org/
[10]台灣高品質學術研究網路
http://www.twaren.net
[11] 台灣網路資訊中心 RPKI 服務系統
https://myrpki.twnic.tw
[12] 台灣網路資訊中心 RPKI Validator
https://validator.twnic.net.tw/roas
[13]Bogon 參考清單
https://www.team-cymru.com/bogon-reference.html