Beware of BGP Attacks

R07944058
網媒碩一 陳鵬宇

1 Summary

本文提出了一種域內路由系統是在自治系統（AS）下運行的，在這種情況下 BGP 協議提供了 AS 之間的連接能力，也就造成了攻擊方可以在域於域之間動手腳。其中探討攻擊者如何利用 BGP 協議來破壞域間路由基礎架構，希望藉由證明 BGP 容易受到大量惡意攻擊，並提高網絡研究界對此問題的意識。

第 2 節 Attack Objective，在黑客已設法破壞、控制互聯網中的一個或多個 BGP 路由器假設下，提到了四種 attack。第一種為 **Blackholing**，當從大部分 Internet 無法訪問 prefix 時發生。故意 blackhole routing 強制加入私有和未分配的 IP 範圍，旨在吸引特定路由器的流量然後「丟棄」它。第二種為 **Redirection**，被破壞的目的地冒充真正的目的地來接收保密信息（破壞 confidentiality），另一個目標可能是將過量的流量重定向到某個網路，導致擁塞崩潰。第三種 **Subversion** 是 Redirection 的特殊情況，攻擊者強制傳輸通過某個 link，目的是竊取修改數據（破壞 integrity），在此情況下，流量仍然被轉發到正確目的地，使得攻擊難以被發現。第四種 **Instability** 是由連續的廣播（可能具有不同的屬性）和同一網絡的提取引起的。這種攻擊可以是在上游路由器中觸發路由衰減，從而導致連接中斷，另一個目標可能是創建 BGP 流量的大量增加，從而導致長收斂延遲。

第 3 節略述了上述攻擊的手段，例如換掉 prefix、false UPDATE 等等，第 4 節說明了一些解法，如 route filtering、S-BGP。

2 Strength(s)

第 4 節的 route filtering 利用可被信任的 ISP 提供域內彼此可被驗證的 database，並檢查 outgoing 和 incoming UPDATE 的訊息是否有被換掉，這樣可以確保 integrity，優點為高速、無加密需求，同時節省體憶體。S-BGP 介紹了 *Address Attestations* (AA) 和 *Route Attestations* (RA)，AA 確保了原先傳送方 AS 是被驗證過的，RA 由 UPDATE 中的 S-BGP 路由器添加，授權相鄰 AS 傳播該 UPDATE 中包含的路由，並且 S-BGP 運用了階層 PKI infrastructure 去驗證 AAs 和 RAs，其中 prefix 的認證內容需由第三方檢驗，所以可以偵測出 compromised router 和正常 router 的區別。

3 Weakness

S-BGP 無法阻止 collusion attack。當兩個已經被攻破的路由器偽造它們之間存在直接連接時，這種攻擊是可能的。其它人看起來就好像兩個 AS 連接在一起。第 4 節提到的兩種攻擊方式都有相對應的 overhead，現在無線網路普及，在 broadcast 的傳輸方式下，我們要怎麼建立信任的 ISP 和 AS，這相對有線的環境很難做到。S-BGP 用到的 hiearchy PKI infrastructure 則是需要大量的計算成本。

4 Reflection

BGP 是一種去中心化自治路由協定。它通過維護 IP routing table 或 prefix-table 來實現自治系統（AS）之間的可連通性，屬於「向量」路由協定。BGP 可以說是 Bellman-Ford 距離向量路由演算法的一個實例。該演算法允許連接設備（BGP speakers）的集合各自學習連接網路的相關拓撲，這很像一個社交謠言網路，每個聽到新的謠言的人都會馬上通知所有的朋友。

Route filtering 和 S-BGP 除了資安上的學術價值外，也能思索如何真的應用到真實世界，像社交系統、Skype 的 super node、區塊鏈等等去中心化的應用，都有使用安全協定的必要性。