SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks

R07944058
網媒碩一 陳鵬宇

1 Summary

DoS 是在資安中一個常見的問題，攻擊方透過大量「合法」、偽造的請求去占用大量的頻寬，以致於伺服器端不能順利的服務那些真的有需求的人，之所以會有這樣的現象是因為接收方無法在收到封包前就預先停止這樣惡意的流量，而當前的機制都需要路由器、ISP 的幫忙才能阻止。

本文提出了 SIFF (Stateless Internet Flow Filter)，它提供終端主機選擇是否讓個別流量到達其網路。通過 handshaking 交換 capability 將流量分為 privileged 和 unprivileged 兩類，SIFF 對傳統 client-server 能達到 transparent，且只有更新過的 hosts 才能享有此優勢。

2 Strength(s)

本文給了詳細的敘述和預先假設，例如：client/server 通過 privileged 的 channel 來溝通，接收方有權利控制流量，在路由器的狀態是小且常數的等等。

Protocol 的設計如下，假設 Client (C) 要和 Server (S) 建立 privileged channel，handshake 的發起者 C 首先發送一個 EXPLORER packet，並初始化 Capability 為 0，Signaling Flag (SF) = true，Packet Type (PT) = NIL。路徑上所有路由器都會左移 z bits 到達 EXP 的 Capability field，在文中有很詳細的透過圖示介紹這部分的運作。

C 要與 S 溝通時，他會沿路將所有路由器的對應的 marking 加入 Capability field，當 C 要再傳 DATA 給 S 時，路由器就會依序確認剛才被他們自己加入 Capability field 的 marking 是否相等，同時這也可以延伸成 window 存值，透過對 packet 進行 window authentication 和 marking。路由器檢查 marking 是否等於其 window 中的一個有效 marking，並始終將 window 中的最新 marking 旋轉到 Capability field 中從而降低下次再查詢的時間。

3 Weakness

論文中提出的方法，可以有效的在接收方還沒收到封包時，就有路徑上的路由器率先檢查，根據不同的 privilege 等級和確認 Capability field 中的 marking 來「事先」有效丟棄掉不需要的封包，但這一來有一個缺點，每個 packet 必需多存這些 error checking 的值，一但路徑中路由器的數量大起來，會有一定的 overhead，slide window 也會增加時間複雜度，若沿路共有 n 個路由器，每個 slide windows 大小為 m，這樣 worst case 會需要 $O(nm)$ 的時間，雖然可擋下一些惡意封包，但所耗費的時間去 check 是否划算也是考量點之一，同時若攻擊方成功傳送了「合法」封包後，他可以開始修改封包中的內容，只要他的 Capability 還沒有被清掉時，就能騙過路徑上的路由器，仍然進行 DoS 攻擊，只是攻擊的時間短了些，因此需要在重複計算 Capability marking 和 marking 的 TTL 中取得平衡。

4 Reflection

DDoS 現在還是個棘手的問題，攻擊者利用了大量的殭屍網路來灌爆另一伺務器系統的連線或處理程式，導致伺服器無法提供服務給其它「合法」流量，而這可怕的地方就在於伺服器沒辦法在端點時有效分辨誰才是「真的合法」，本文提出的 SIFF 提供了一套機制讓路徑上的路由器也參與這「審查合法性」的能力，但若路由器端已經被攻擊者給攻破，這樣就會很像 TOR 有幾個節點已經產生漏洞了，接收方還自信滿滿的覺得只要被「我所信任的路由器」所檢查過的封包，都是合法可以被傳送的，殊不知當幾個路由被控制時，這樣的方式也不安全，而定期分配新的路徑和路由可能是個有效的解法，降低攻擊者預測哪些路由器是檢查方，從而降低被控制後，再 DoS 攻擊的可能性。