Tor: The Second-Generation Onion Router

R07944058
網媒碩一 陳鵬宇

1 Summary

這篇論文提出了一種新一代的路由器：Tor（洋蔥路由器），Tor 是一種基於電路的低延遲匿名通信服務。第二代洋蔥路由系統通過添加完美的 forward secrecy、congestion control、directory servers、integrity checking 及通過 rendezvous points 實現位置隱藏服務的實用設計來解決原始設計中的限制。

整個 tor 架構的設計目標有以下幾點：babel、mix-master 和 mixminion，目標是達到較大和可變的延遲為代價去實現匿名；Anonymizer 易於分析，但用户必需要信任匿名代理人；Crowds 任何節點都可以讀取用户的流量；Herbivore、P5 這是透過 broadcast 來隱藏發起者。

2 Strength(s)

洋蔥路由器在匿名性、可用性和效率之間取得了很好的平衡，實現整次對話傳輸兩端的發送者和接收者被匿名保護。另外，在文中提到了引導洋蔥路由器的演變目標共有以下幾點：可部署性、可用性、靈活性，還有很重要的一點：簡單好實現的架構，這些都是洋蔥路由器的優點。

每個洋蔥路由器都與每個其它洋蔥路由器（OR）保持 TLS 連接。每個用户執行稱為洋蔥代理（OP）的 local 軟體來獲取目錄，在網路上建立起電路，以及處理來自用户應用程式的連接，這些 OP 接受了 TCP 流並在電路中復用它們。電路另一側的 OR 連接請求的目的地的中繼數據。OR 維護共有兩個金鑰，一個是長期身份所用到的一般金鑰，二是短期洋蔥金鑰。

3 Weakness

用户指紋辨識上的議題，每個用户在瀏覽網頁時的習慣是不同的，例如螢幕尺寸大小、當地時間、甚至是滑鼠滾輪的速度，這些資訊構成了一個用户的指紋。Tor 可以禁止讀取瀏覽器相關資訊來阻止用户隱私的洩露。

誹謗攻擊：攻擊者可能因為不贊成某個人的行為，想要汙名該人，去使用洋蔥路由器網絡，給他帶來壞的名聲，使得被攻擊者被停止服務，但出口退出策略能夠一定程度減少這種濫用的可能性。

破壞目錄服務器：如果有一些目錄服務器突然消失了，其他的目錄服務器仍然運作著時，還活著的目錄服務器可以共同決定一個新的有效目錄，只要任何目錄服務器仍在運行，它們將生成一致目錄並廣播去告訴大家，但若是剩下的人都是惡意的，而消失的人就喪失了這輪的投票權，就會變得危險。

4 Reflection

看完這篇論文後，在 Google 上查詢了有關的應用，有看到一個很有趣的東西叫 Tor Browser，Tor Browser 是個內建翻牆功能的瀏覽器，藉由洋蔥路由器的匿名瀏覽技術，將上網時所傳遞的訊息層層加密保護，讓使用者在瀏覽網站時不被監控或側錄，也無法查處原本的 IP 位址或追　真實的使用者身份。

在安全之餘，也有一些相對應的議題隨之產生，例如這樣速度就會一定程度的受限，在看高畫質會需要流量較大的服務就會比較不適合，但好處就是安全性獲得了保障。

可以知道，洋蔥路由器提升了安全性，但限制了頻寬流量，這也讓我連想到第一週的那篇論文，如何在 security 和 usability 之間做考量，或許網速變慢不能完全比擬成是 usability 變差，但概念上都是在安全性與另一者之間做取捨。