撰寫：資管三 B04705001 陳約廷
日期：2018.04.10
標題：Reading critique —— Tor: The second generation onion router

---

Summary

在這篇論文發表以前， Onion Router 是作為匿名連線的一個重要方法。而 Tor 就是針對這個做更多的改進。而在 overview 時對提出的模型做了前提，刪去多餘的考量，為了簡化模型目標使得改進的目的變得明顯。
Tor 有以下的特色：

- 分散式的 congestion control 使得流量可以被控管。但這個僅指於正常使用的狀況，文章後頭也表明並沒有辦法預防 DDoS 攻擊
- 設立 Directory server 作為連接點展開匿名化
- 增加點對點的完整性檢查，這是第一代 Onion Router 所沒有的，能被竄改封包是一件很嚴重的事，因此 Tor 對此做出改進。
- 原本第一代建立連線之後會有 reply onion 來與中繼點連線，但是在連線的變化中 reply onion 需要無法被更動，因此 Tor 刪去 reply onion ，改設立一個會合的 node 建立連線。

再來論文對現有的設計做一個簡介，目的應該是要列出在不同的 layer 如何匿名化。來顯示 Tor 的匿名化是混合式的，可以在傳輸層以下匿名化。

Tor 是設計來給廣大的網路世界使用的，因此在 Design and Assumptoin 就提出了這樣設計的限制與條件。威脅模型的部分僅設定攻擊者想要分析封包，也就是 Tor 需要預防封包能夠被完整的分析。

Strength(s)

- 提出使用者的使用情況，使設計的目標明確
- 從前提、設計目標、主要設計、可能攻擊、以及初步經驗，架構完整詳細
- 對可能攻擊有完整的介紹

Weakness(es)

- Overview 裡頭就大量的介紹了 Tor ，或許應該到後續 Section 再提，脈絡比較清楚
- 對現有設計的介紹過於冗長。
- 對 Threat Model 過於簡陋，卻又在最後描述各種 Attack 的地方提到一大堆不安全的地方
- Directory server 是可被攻擊的點
- 用來驗證完整性的 SHA1 已被攻破，因此需要更新完整性的驗證協定

Reflection(s)

作者可能是想要盡可能的詳細介紹 Tor ，所以把太多東西一次講完，使得論文有點難讀，或許可以用額外一篇以分析 Tor 為題的論文來把東西分開來講會使得論文的結構更簡潔。