撰寫：資管三 B04705001 陳約廷
日期：2018.05.14
標題：Reading critique —— Maneuvering Around Clouds: Bypassing Cloud-based Security Providers

Summary

這篇論文介紹如何突破 CBSP 來找到伺服器的真實 IP ，藉此可以來對伺服器進行 DDoS 攻擊。首先介紹 CBSP 的機制，是由伺服器送到雲上，使用者的要求會先經過雲轉送到伺服器，藉此來保護伺服器的真實位址。

但是這樣的機制仍然有許多漏洞，論文裡列出了許多項。

- 系統工程師可能會想在 subdomain 下設定一個後門好方便直接連接伺服器，這樣可能存在風險使得 subdomain 被發現而使得真實 IP 曝光。
- DNS 記錄仍然存在，如果是存在於網路上的網站，可能會被用 dig 挖出真實的 IP。
- 如果 cloudbase 暫時中止時伺服器仍然在線上，那麼會被 dig 出真實 IP 。
- html檔案中可能有對 server 資料庫的 request ，如果並沒有所有東西都進行 redirect ，則會暴露真實 IP 。
- 就算經過 redirect ，但是數位憑證仍然是由跟真實 IP 底下的數位憑證是一樣的。因此如果使用掃描工具暴力搜尋 IP 並比較數位憑證，就還是可以被找出真實 IP 。現在使用 zmap 已經可以在 45 分鐘內掃描整個網路，這也代表 CBSP 根本不是有效防禦 DDoS 的方法。

再來是對現有的 CBSP 的 survey，統計上述的攻擊方法下有多少部分的網站是可以被 DDoS 攻擊的。

Strength(s)

- 主題是與網路實際應用相關的，而提出的方法都是真實有用的
- Introduction 很詳細的描述目前環境與問題，使得論文很好讀

Weakness(es)

- survey 中統計的百分比數並沒有實質的意義，使篇幅過長
- 在各種攻擊方式處，僅概述攻擊方法

Reflection(s)

這篇論文把攻擊 CBSP 的方法都集中起來發表，提高了大家對 CBSP 不安全性的警覺。如果我是作者，我會把統計的部分再精簡，因為其實百分比那張圖就已經足以警告大家自己身陷危險之中。然後提出 attack 的步驟，使攻擊的描述更具體。