撰寫：陳約廷
日期：2018.04.22
標題：Reading critique—— Beware of BGP Attacks

Summary

論文是屬於 attack and analyze 型的論文，不過是屬於精神式的攻擊。首先假設攻擊者已經完全掌控其中一台網路中的 BGP router。攻擊者試圖想要對網路中的連接者與 BGP 路由器做各式各樣惡意操作。基本上在 BGP 是一個純粹為了 Routing 而存在的協定當中，如果伺服器被攻擊了，基本上整個網路就落入攻擊者的魔掌中了。

因此在接下來 Attack Mechanism 中的那些攻擊都可以被有效的執行，原因是 BGP 完全沒有對惡意使用者的防護。在 Integrity，Confidentiality上都沒有下太多功夫，僅僅是滿足 Availability。

再來提到現有在 BGP 上所做的額外防護。BCP 說實在的不算什麼防護，就是一個提醒文件。 Route filtering 可以設立名單來檢測收發 update 時的 peer，但是由於更新並不頻繁所以並不十分有效。S-BGP 算是裡面最安全的，因為在 router 之間的連線要有嚴謹的簽證，但是卻有會使得效能不佳的副作用。

最後論文再重申一次想要增加大家對 BGP router 危險性的意識。

Strength(s)

- AS topology 用圖來表示清楚
- 子項目分的很清楚，也有助於翻閱論文
- 論文結構完整，攻擊、攻擊的防護、未來的發展中，是個清楚的 attack and analyze。

Weakness(es)

- 攻擊的流程都是大量的文字，缺乏符號與圖案表示

Reflection(s)

我覺得論文對 BGP 攻擊的進行得非常順利，因為 BGP 被設計時就沒有把資訊安全這個領域納入考量之中，設計出了良好的傳輸協定但沒有保護它。或許如果要達成資訊安全不應該是在 BGP 上，因為他就是個 Routing protocol。應該要從 Data packet delivery 做起。畢竟傳輸也是一個封包一個封包於路由器之間傳送，那麼從 packet delivery 方面研究才比較有可能達成 integrity 這個性質。畢竟 BGP server 隨時有可能被控制，因此 confidentiality 應該難以達成，況且如果是想要有保密性，那應該用更安全的傳輸方式才對。