撰寫：陳約廷
日期：2018.03.14-2018.03.19
標題：Client puzzles: A cryptographic countermeasure against connection depletion attacks

Summary

過去DDoS是一個著名的攻擊手段，駭客利用強大的電腦不斷送Request給伺服器，導致伺服器忙用接收Request而癱瘓。當時現有的防禦手段有 time-out、random dropping、syncookies，但是各有各的弊病。time-out會使正常使用者暫時中斷、random dropping 只是個治標不治本的作法因為只是限縮處理的要求數量、snycookies無法防止內網中的入侵者。

論文提出了一個全新的協定。在與伺服器建立之前必須先解決伺服器提供的謎題，這個需要計算但是計算量對正常使用者來說並不是大量。但如果想要用DDoS攻擊伺服器的話就需要非常大量的計算。因此這樣的協定可以有效的防止DDoS的攻擊。

Strength(s)

在引言中調查了現有的所有防禦手段與弊病，讓讀者清楚知道現階段受到DDoS攻擊所面臨的種種問題，也有助於接下來提出的協定。

論文非常明確的是要建立一個能夠防禦DDoS的協定，因此論文清楚地設定了安全系統所需要的要素——Attack Model。對攻擊者有非常完整的瞭解與設定。Section 2 中的 Attack Model 中設定攻擊者無法攔截並更改封包，但可以用任何IP來連結伺服器。

在協定中清楚的用代數還有示意圖描述了協定內容，對瞭解協定有幫助。先完整描述了一個puzzle的建立與複雜度，再來討論伺服器的緩存大小與連結欄位的數量設定。整個協議很簡單明瞭，也很容易理解卻很有效。作者也沒有避諱把副作用說出來，說這樣的協定會減緩連結速度。最後在附件也有附上對提出理論的完整數學證明。

網站在這樣的協定下可以擁有合理大量的正常使用者並維持一定的效能。

Weakness(es)

當然在設定好的攻擊者模型之下可以有效地防禦攻擊，但是永遠沒有100%的防禦。一旦攻擊者擁有協定中的攻擊者所不具有的能力，這個協定就可能被突破。

計算能力會不斷的演進，因此puzzle與buffer size 的設定要一直與實漸進。如果有些老舊的機器並沒有更新過去的Client Puzzles Protocol，仍然可以被現有的強大電腦破解。

Reflection(s)

這篇論文根本就是個範本。提出有效的資安防禦協定，結構完整嚴謹，且描述詳細。希望我以後也可以寫出這樣的好論文。