Critique 10: b07902127 資工二 羅義鈞

Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attack

Summary:

本篇提出以 client puzzle 的方式解決 Connection Depletion Attack，經典的代表就是 TCP SYN flooding。作者比較了傳統上使用 syncookie 的方式與 client puzzle 的優劣，並建立好 Attack module, 對攻擊者作出五點的 assumption。接著建立 Client Puzzle Protocol, 標註其需要的 notation 以及 parameters、sub-puzzle 等數學說明。作者也比較一般情形與遭受攻擊時 Protocol 的應對方式，並且以數學分析 client (or adversary)要解決 puzzle 的 cost 是多少：由於有 m 個 sub-puzzle, 假設每個長度為 k-bits，最多的計算量就是 $m \times 2^k$。而 server 會先去檢驗時間是否過期，才做 puzzle 的認證。透過讓 client 解 puzzle，可以有效降低攻擊者的 DoS 目的。而作者也考量了一種情形：攻擊者可以利用讓 server 不斷的製造發送 puzzle 與驗證 puzzle 而導致 server 資源的消耗。作者用 buffer size 來處理這個問題：藉由開大小為 maximum connection + b slots，只要 $b > (\text{number of time steps for attack})/(m2^{k-1})$，攻擊者要成功達成 Connection Depletion Attack 就得花上過多的時間在解決 puzzle。

Strengths:

1. 和傳統的 syncookie 相比，client puzzle 少了這項 assumption: 攻擊者無法攔截 message sent to spoofed IP address。由於這項 assumption 常常是錯誤的，攔截封包並不是那麼的困難，因此跟一般的 syncookie 相比，client puzzle 有此優勢。
2. 對應攻擊者的攻擊強度，可以去調整要解 puzzle 的 bits 數來對應，彈性比較大。
3. 對於額外需要的 buffer 以及 assumption 皆有說明清楚，並且用數學做說明。

Weaknesses:

1. Client 需要有解 puzzle 的軟體，否則就無法進行連線。
2. Puzzle 需要佔用 client 的運算資源，一旦系統遭受攻擊，client 需要進行更多運算。
3. 攻擊者如果夠有耐心持之以恆的攻擊，可能會運氣好遇到 puzzle 好解決的時候，而成功進行大量的連線。

Reflection:

這個做法可以有效阻止 Connection Depletion Attack，尤其是當 attacker 有能力去快速的執行 connection depletion。可以延伸的研究方向是 puzzle 的效率問題，如果因為 puzzle 讓一般的使用者運算資源被浪費掉，會對一些運算能力較弱的使用者不公。由於這篇文章抵擋的攻擊是容易實現且效果顯著的，除此之外還能用於其他用途(ex. conjunction with dropped connection)，因此可以讓很多 server 受益，免於類似的攻擊。