Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks

✧ Summary

本篇旨在利用 cryptographic puzzles 以對抗 **connection depletion attacks**。Connection depletion attack 為一種 denial-of-service(DoS)攻擊手法，包含 TCP SYN flooding、e-mail bomb attacks、或是利用 SSL 協定特性、FTP 讀取或寫入大量資料來耗盡伺服器資源(如:儲存空間、記憶體、頻寬)，令一般合法使用者無法正常與伺服器溝通。

當中，TCP SYN flooding 攻擊手法為利用 TCP "half-open" 的特性，攻擊者便可發起大量連線，但不回應最終的 ACK。而因為伺服器 buffer 有限，記憶體皆被這些無效連線塞滿，最後伺服器便無法再回應 TCP 請求。而若攻擊改為利用 SSL 協定，則情況可能會更嚴重，因為伺服器計算 public-key-based decryption 是相當費工的，因此伺服器的運算資源很可能被這些無效的 SSL 連線給用盡。

為了解決 connection depletion 問題，作者提出" **client puzzle**" protocol 解決方法：在伺服器未遭受攻擊時，將會正常接受連線。而當遭受攻擊時，伺服器將只選擇接受能把 client puzzle 於時間內正確解開並回傳的連線，否則便不為其保留資源。

✧ Strengths

Client puzzle 相較於傳統的 time-out approach、random dropping approach、syncookie 等方法還要佳，在比較強的 attack model 中能較為 robust。因 Client puzzle 不會像 time-out 方法需要尋找最佳的設定(太短正常使用者會無法連線;太長攻擊者加快速度仍可將 buffer 佔滿)，也不像 drop 方法在攻擊速度高時會隨機丟掉許多很法的連線，也不用如 syncookie 一般需要假設 message 不會被攻擊者截取，且 client puzzle 還能對抗 IP spoofing。此外，client puzzle 的彈性較大，當攻擊速度變強變快的時候，僅需要增加 puzzle 難度便可提升難度。不僅如此，client puzzle protocol 能與其他方法共同整合，在現有的 protocol 上也較易部署(syncookie 或 drop 方式皆須要在伺服器端上對 service protocol 進行修改)。

在另一方面，puzzle 為 stateless 的，且容易驗證，因此不會有大量 query 反而使資料庫遭 DoS。除此之外，client puzzle protocol 可以允許匿名連線且不需要 PKI，而即便在重度攻擊情況下，也不需要進行 retry。

✧ Weaknesses

這其中最大的麻煩便是在 client 端需要額外安裝 special-purpose software(如:瀏覽器 plug-in)，才能用以解開那些 puzzle。另外，若於今日世界中，恐怕 puzzle 長度需相當長才較能有效果，但這也意味著一般正常使用者所需計算、等待回應的時間也較長，伺服器所需驗證的時間也較長。倘若攻擊者的運算能力甚至遠超過老舊伺服器者，可能伺服器也會忙於驗證大量 puzzle 的正確性，而正常使用者便有可能遲遲等不到伺服器確認。又或者可藉由攻擊伺服器其他已開啟的 port，而也可令伺服器忙於回應其他 request，使之成為某程度意義上的 DoS。

✧ Reflection

Cryptographic puzzles 尚可用於對付 junk e-mails、創造 digital time capsules、測量 Web site usage 等，然而隨著運算能力不斷進步甚至是量子電腦的出現，此種 Cryptographic puzzles 方式可能每隔一段時間就需要重新檢視、修正一番。

時至今日，很多 DoS 或 DDoS 手法為攻擊 decoy 或 backbone，也一樣可令伺服器無法正常回應，未必僅有 overload 伺服器的方式。此外，很多時候可能是反彈放大攻擊，甚至可以**請殭屍網路中的 bots 來發出請求並解開 puzzle**，因此若欲於今日環境中部署，或許仍有許多需要改良的地方。

最後，安全性與效率難以兼得，為了防堵 connection depletion attacks 可能會犧牲一些使用者體驗，甚至令使用者不耐煩、反感，依然可能會流失客戶，因此怎麼選取平衡點也是網站管理者需考量的議題之一。