B04902103 資工四 蔡昀達

Reading critique #8

Paper : A. Juels and J. Brainard, “Client puzzles: A cryptographic countermeasure against connection depletion attacks,” in NDSS, 1999.

1. **Summary**

   This paper introduce a new counter measurement to defend connection depletion attack. It utilize complexity difference between client and server side. When the buffer on the server is about to full, it request the client to solve puzzle to stop attacker from redundant connections. The puzzle can be scaled up and parameterized according to the condition when under attack. This method has several assumtions which limits it only to connection depletion attacks.

2. **Strength of the paper**
   1. The method is still secured when the attacker can intercept messages therefore useful for defending against interal attacks where syncookie approach fails.
   2. The client puzzle protocal can handle higher spped attacks compared to dropped connection approaches.
   3. The size of puzzle can be adjust dynamicaly making it very flexible.

3. **Weakness of the paper**
   1. This approach requires special software on the client side.
   2. This approach will not work and the server will still be saturated when the attacking speed is too high.
   3. This approach may penalize innocent connections when there are attacks in the same time.
   4. It seems that it lacks pratical experiments to prove their theory.

4. **My reflection**

   This counter measurement are very similar to the merkel puzzle introduced in the public-key cryptosystem. It has several assumtions and limitations but its concept of utilizing complexity difference between client and server side is very useful.