B04902103 資工四 蔡昀達

Reading critique #9

Paper : S. Frolov and E. Wustrow, "The use of TLS in Censorship Circumvention," in NDSS, 2019.

1. **Summary**

   Unique TLS implemetation can be easily distinguished and therefore circumvention tools can be easily detected and blocked. This paper collects billions of TLS traffic and analyzed censorship circumvention tools to determined ones at risk. Mimic popular TLS implemetation isn’t easy. This paper intoduced a library, uTLS, that allows developers to easily mimic popular TLS implemtation and protect circumvention tools.

2. **Strength of the paper**
   1. This paper collects and open their billions of TLS traffic data.
   2. The authors developes uTLS library to help easily and automatically mimic populer TLS implemetation and uTLS is integrated by many circumvention tools.
   3. uTLS also support many features such as fake session tickets, multiple fingerprints, randomized fingerprints which are very useful.

3. **Weakness of the paper**
   1. The dataset are not absolute complete because of packet loss due to network traffic congestions.
   2. The analysis only contains TCP packets.

4. **My reflection**

   Before reading this paper, I thought that using TLS could be very safe. Anonymity tools like Tor can also benefit and can conceal our identity. However, these can be can easily detected by TLS fingerprints. Security are so diificuilt to achieve because protocols in all internet layers have to be carefully designed.