B04902103 資工四 蔡昀達

Reading critique #6

Paper : D. Fifield, C. Lan, R. Hynes, P. Wegmann, and V. Paxson, “Blocking-resistant communication through domain fronting,” in Privacy Enhancing Technologies, 2015.

1. **Summary**

   This paper intorduce Tor, the second-generation onion routing system. This system aims at providing anonymity and gives several improvements from the origin design including integrity check, variable exit policies, congestion control, one curcuit for multiple streams. It uses cells to communicate and the IP cannot be tracked.

2. **Strength of the paper**
   1. Tor is perfect forward secrecy
   2. Change tracks with variable exit policies

3. **Weakness of the paper**
   1. Very few Tor uses https
   2. It can be tracked by observing traffic pattern since it is low-latency
   3. End nodes would be targeted by attackers and reveal every imformation if compromised
   4. Slow when circuit is long.
   5. Can be easily blocked by blocking the directory servers.
   6. Not suitable for P2P

4. **My reflection**

   The design of Tor provides much anonymity, but still there are many problems that can leak the user information. There are many new methods such as Garlic routing, Herd, Vuvuzela/Alpenhorn, Dissent, etc that improves even greater. Maybe using connections like VPN + Tor can meet a even higher security demand.