B04902103 資工四 蔡昀達

Reading critique #4

Paper : L. S. Huang, A. Rice, E. Ellingsen and C. Jackson, "Analyzing Forged SSL Certificates in the Wild," 2014 IEEE Symposium on Security and Privacy, San Jose, CA, 2014.

1. **Summary**

   This paper analyzed forged SSL certificates in the wild from real world data. It proposed a method to detect the occurrence of man-in-the-middle attack. It also dicuss the limitations and some prossible defenses.

2. **Strength of the paper**

   It is the first paper to conducted analysis on forged SSL certificates and come up with a novel method to detect man-in-the-middle attacks. It shows results from real world data and provide hard evidence of malicious activities. These analysis gives us the insight to find suspicious certificates.

3. **Weakness of the paper**

   This paper assumed most browsers support flash player plugins. The detecting methods can be easily blocked or evade as long as the attacker is fully awared of the detection methods. As metioned in the paper, websites nowadays could simply detect attacks with their native mobile applications.

4. **My reflection**

   Most browser nowadays blocks or do not support flash player plugins becuase of its own security problems. Detecting man-in-the-middle attack with flash player plugin may not be an option anymore. The paper metioned that users often ignore SSL certificate warnings. Even with risk awareness, I always connects to my own server which uses self-signed certificates. Not suprising that usability again beats security. Human factors would be the most difficult problems to solve.