B04902103 資工四 蔡昀達

Reading critique #3

Paper : A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," in RSA CryptoBytes, 2005.

1. **Summary**

   This paper intoduces TESLA, a broadcast authentication protocol which achieves asymmetric properties. It has low computation and communication overhead, limited buffering, robustness to packet loss by one-way chain, scales to large number of recievers. The assumptions are that by using secure PRF with loosely time-synchronized, it would be computationally intractable. And a time stamping server can achieve non-repudiation.

2. **Strength of the paper**

   This protocal has several advantages. It is low computation and communication overhead, limited buffering required, strong robustness, sacles to large number of recievers which solves most challenges in source authentication.

3. **Weakness of the paper**

   Authentication at receiver is 1. Check if packet is in legitimate time interval 2. Check if the key is already disclosed 3. checks the legitimacy of the key. Without checking if the key index is reasonable or not (may be extremely large), it could be easily attacked.

   This protocal does not consider DDos attacks such as reviever buffer flooding.

4. **My reflection**

   There are some extensions in further publications which provide some features to enhance this protocal in “A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast", Network and Distributed System Security Symposium, NDSS '01, p. 35-46, February 2001”. Including tight lower bound on the disclosure delay, immediate authentication without buffers and reduce overhead by concurrent TESLA instances.