SENG2250/6250 System and Network Security

School of Electrical Engineering and Computing

Semester 2, 2020

Lab 11: Solutions

1. What are the two security protocols defined in IPSec?
   Authentication Header (AH) and Encapsulating Security Payload (ESP)

2. What are the security services provided in IPSec?
   Basically, source authentication, message authentication/integrity check, data confidentiality and access control.

3. Can we use IPSec to protect the MAC information of a user?
   No, because IPSec works on the network layer which is higher than the MAC layer.

4. What are the IPSec transport mode and tunnel mode, what are the differences?
   Transport mode can protect most of IP packet other than the original IP header. Tunnel mode is able to protect the entire IP packet.

5. Why does ESP include a padding field?
   For block cipher encryption and the use of operation modes.

6. What is a security association?

   SA is a simplex (unidirectional), logical connection that provides security services to a traffic steam between two IP nodes.

   An SA serves as a contract between two or more entities and completely specifies how they use security services to communicate securely.

7. –
8. What information should be contained in an ISAKMP SA?
   An SA specifies a number of parameters, such as the AH authentication algorithm, the ESP encryption algorithm, the ESP authentication algorithm, keys, IVs, IPSec protocol transport or tunnel mode and lifetime.

9. What is about the IEEE 802.11i standard?
   IEEE 802.11i is to address the identified security weaknesses for both authentication and encryption protocols.

10. What security issues of WEP are addressed in TKIP.
    Shot key size issue; integrity checking.