11210/IIS500200 Network Security

Final

Instructor: Prof. Amir Rezapour

1. True or False? **Explain why**? (50 points)

   (a) Suppose an opponent captures an unexpired service granting ticket and modifies its network address to match that of the valid user. Is it correct that the opponent will be granted access to the corresponding service.

   (b) If the lifetime stamped on a ticket is very short (e.g., minutes) an opponent has a greater opportunity for replay.

   (c) User certificates generated by a CA need special efforts made by the directory to protect them from being forged.

   (d) In IPsec, authentication must be applied to the sections of the original IP packet.

   (e) The principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level.

   (f) A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall but also records information about TCP connections.

   (g) Packet filter firewalls examine upper layer data therefore they can prevent attacks that employ application specific vulnerabilities or functions.

   (h) The change cipher spec protocol exists to signal the transition in ciphering strategies.

   (i) Transport mode in IPSec provides security to the entire IP packet.

   (j) In tint fragment attack, it is possible for an intermediate fragment to pass through filter before the initial fragment is rejected.

2. Suppose Alice has a secret a and Bob has a secret b. Alice and Bob also have access to a secure communication channel. The goal is to let a server s compute $sum = a \oplus b$. However, they don't want s learn a or b. How can they achieve this. (10 points)

3. Consider the following protocol:

$$\begin{aligned} A \to KDC &: ID_A || ID_B || N_1 \\ KDC \to A &: E(k_a, [k_s || ID_B || N_1 || E(k_b, [k_s || ID_A])) \\ A \to B &: E(k_b, [k_s || ID_A]) \\ B \to A &: E(k_s, N_2) \\ A \to B &: E(k_s, f(N_2)) \end{aligned} \tag{1}$$

   (a) Explain the protocol. (5 points)

   (b) Can you think of a possible attack on this protocol? Explain how it can be done. (5 points)

(c) How can we prevent this attack? just write the basics of the idea. (5 points)

4. IPSec documentation allows combining the security associations. Discuss why is it recommend to perform ESP protocol before AH protocol? (10 points)

5. What are the different types of port forwarding supported by SSH? Give an example for each type. (15 points)