CS5285: Information Security for eCommerce Sem A, 2024/25
Tutorial 11, Week 13 (December 3) Gerhard Hancke

Question 1 IPSec

(a) How many different methods are there if two hosts would like to authenticate packets between them?

(b) Can you think of an advantage of transport mode over tunnel mode if only authentication is required?

(c) Can you think of a reason why in transport mode AH could be slightly better for authentication than ESP?

(d) What is the purpose of padding when using ESP?

(e) Discuss advantages/disadvantages to IKE main and aggressive mode.

Question 2 WiFi

a) You are using WEP to secure your WiFi connection.

i) Attackers can gain knowledge about the plaintext of the message if the keystream happens to repeat. You are sending 10,000 new WEP messages, on average, every second. How long does the attacker need to wait for the keystream to repeat?

ii) An attacker knows the plaintext of one of your messages. How can he modify the message so the receiver receives and accepts his new message?

b) You wish to use public WiFi at the shopping mall but it is set up to use WEP. What can you do to ensure you have improved security for your connection?

Question 3 Mobile

a) What basic security services does a 2nd generation mobile network provide?

b) What basic security services does a 3rd generation mobile network provide?

c) Consider the simplified 3G system shown below. Construct a suitable protocol and explain how mutual authentication is achieved.