CSE 473 – Introduction to Computer Networks

Quiz 5

Your name: *11/12/2013*

1. (4 points). Consider a block cipher with a block size of 8 bits that is used to encrypt English text, represented by ASCII characters. Assume we augment this with cipher block chaining. So, the first byte is xor-ed with an 8 bit initialization vector before encrypting it and each subsequent byte is xor-ed with the previous ciphertext byte before encrypting it.

   Explain the purpose of cipher-block chaining.

   Describe how you could break this encryption system. Be specific.

2. (6 points) In a typical SSL session between a client and a remote server, how does the client verify that it is communicating with the desired server, rather than some intruder? Be specific.

Suppose that an intruder removed a record from an SSL packet sent from the server to the client. How would the client's SSL software detect that something is wrong? Be specific.

Suppose an intruder sent a TCP FIN packet to the server that looked like it came from the client. Would this cause the TCP connection to be closed? If so, how would the SSL software detect that something was wrong. Be specific.