EECS 489 – Computer Networks
HOMEWORK 3

DUE DATE Wed, 4/21/2010, midnight.

Leave outside 4629 CSE or email zmao@umich.edu

QUESTION 1

Is it possible for a CDN (Content distribution network) to provide worse performance to a host requesting a multimedia object than if the host has requested the object from the distant origin server? Explain.

QUESTION 2

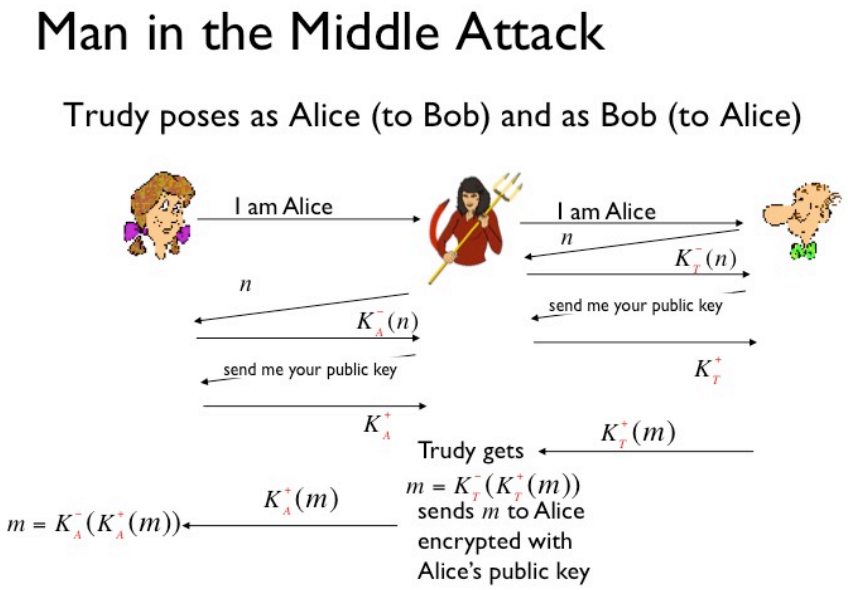
(1) What is the difference between end-to-end delay and packet jitter? What are the causes for packet jitter?

(2) Why is a packet that is received after its scheduled playout time considered lost?

(3) Are the TCP receive buffer and the media player's client buffer the same thing? If not, how do they interact?

QUESTION 3

In the man-in-the-middle attack described in the lecture notes and reproduced here below, Alice has not authenticated Bob. If Alice were to require Bob to authenticate himself using the public key authentication protocol, would the man-in-the middle attack be avoided? Explain your reasoning.



QUESTION 4

Suppose Alice wants to send an email to Bob. Bob has a public-private key pair ($\mathbf{K}_B^+$, $\mathbf{K}_B^-$), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H( ).

(1) In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.

(2) Is it possible to design a scheme that provides confidentiality for ending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.

QUESTION 5

Suppose Alice and Bob are communicating over an SSL session. Suppose an attacker, who does not have any of the shared keys, inserts a bogus TCP segments into a packet stream with correct TCP sequence numbers, checksums, IP addresses, and port numbers. Will SSL at the receiving side accept the bogus packet and pass the payload to the receiving application? Why or why not?