Fall 2010 – CS 686 Security and Privacy
Assignment 3 - due by 11:59pm on Wednesday, Nov 24.

Problem 1: IPSec, which mode? (25 points) 1. IPSec has two modes, Transport and Tunnel. For each attack below, answer which mode(s) can defend against this attack, if any mode(s) can, or none of the above if not. Explain your answer, including where IPSec needs to be installed among sender, receiver, sender gateway, and receiver gateway in the Figure 1 below.

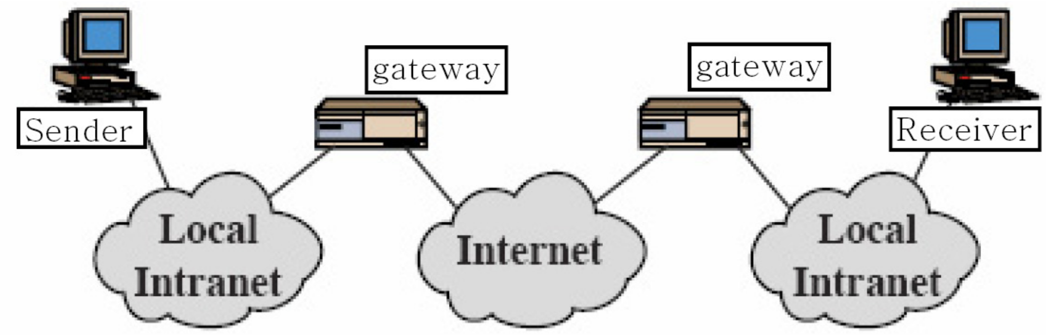

Figure 1: A sample configuration

Problem 1a (5 points) An attacker between gateways records packets in transit to find sender and receiver of certain flow.

Problem 1b (5 points) An attacker between gateways records packets in transit to find content of certain communication.

Problem 1c (5 points) An attacker in the same intranet as the sender records packets to find the receiver.

Problem 1d (5 points) An attacker in the same intranet as the sender impersonates the sender.

Problem 1d (5 points) An attacker in the same intranet as the receiver also receives the packets and find content of any communication coming to the receiver.

Problem 2: IPSec, which extension? (25 points) IPSec has two extensions to the original IP header, Authentication Header and Encapsulating Security Payload. For each attack above, explain which one defends against each attack, if any can, or none of the above if not. Explain your answer. (Write your answer separately as 2a, 2b, ... , 2d.)

Problem 3: Carol's IKE (15 points) Carol decides to study IKE with the course slides, and read up to "Almost-IKE" protocol on slide 17. Then she found out that B(Bob) needed to remember a secret value b for each connection, which leaves the defense against DoS attack not quite perfect despite using hashes. She changes the protocol as follows:

$A \to B : g^a, A$

B computes $b = hash_{Kb}(g^a, A)$

$B \to A : g^b, hash_{Kb}(g^b, g^a)$ and now B forgets b

$A \to B : g^a, g^b, hash_{Kb}(g^b, g^a), Enc_K(sig_A(g^a, g^b, B))$

B computes $b' = hash_{Kb}(g^a, A)$, and computes $g^{b'}$.

If g^b that A sent is the same as $g^{b'}$, then B proceeds.

$B \to A : g^b, Enc_K(sig_B(g^a, g^b, A))$

Carol argues that this is as secure as the original protocol since the $hash_{Kb}(g^a, A)$ cannot be computed by anyone but Bob, as Kb is a secret. Would you agree with her or disagree? Explain your answer.

Problem 4: Overflowing (15 points) Present an attack scenario using buffer overflow, and show two defense mechanisms that can prevent this attack from happening. Explain why these defenses would be effective.