TAKE HOME EXAM – CSCE 813
TEST 1
Fall 2006

RETURN (hard copy) BY October 5, 2006, 12:30 pm

Name:
e-mail:

You may use any materials to answer the questions, however, you need to present the answers in you own words. Include all URLs, references you used for each answer. Staple all papers before submitting.

This must be individual work!

Warm Up

1. (*10 points*) Describe the **advantages and disadvantages** of providing security at different layers of the TCP/IP protocol stack. – max. ½ page

2. (*15 points*) The IPSec architecture document states that when two transport mode security associations are bundled to allow both AH and ESP protocols on the same end-to-end flow, only one **ordering of security protocols** seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption? – max. ½ page

Let's get serious

3. (*15 points*) **Point-to-Point Tunneling Protocol** – max. 1 page
   a. (5) Describe the goal of and the services provided by **PPTP**.
   b. (10) Show an **attack against one of the authentication methods** supported by MS-PPTP.

4. (*35 points*) **IPSec Key Management** – max. 1½ page
   a. (5) Briefly explain the **phases of IKE**.
   b. (10) Describe the **differences** between the base (main) exchange and the aggressive exchange of ISAKMP.
   c. (10) Show that the **Diffie-Hellman key exchange with authentication** is vulnerable to **denial-of-service** attack.
   d. (10) Outline a **solution** for protect against the above problem.

5. (*25 points*) When encrypted traffic must passes through a firewall, e.g., via a connection from a firewall protected LAN to the outside, both the signed message and the signature is encrypted, therefore creating a problem to the firewall to authenticate the message. However, the firewall cannot access the signature without the encryption key used for the communication. Propose an **architecture** that support authenticated communication through an **application-level firewall** that has the following properties:

   a. Signature can be verified by the firewall.

   b. Signature can be verified without access to the plain message content.

   c. Cost of signature verification is not more expensive than the verification by the end user.

   – max. 1 page

BONUS

(5 points)

Explain how IPSec provides limited **hiding of the end-points' identities**.

– max. ½ page