CSC 774 – Network Security

Mid-Term Exam #1
4:10pm – 5:00pm, February 12, 2004

Student Name:_____ Score: _____

You are allowed to use your textbook and notes; however, you are not allowed to exchange anything before you get permission from the instructor. Note that none of the questions need long answers. Please be brief. DO NOT write anything irrelevant to the questions.

Questions 1 – 4. Multiple choices. (Total 40 points. 10 points/question.)

Choose one appropriate answer for each question and write it on the blank below the question.

1. Consider the PayWord micro-payment system. Assume user U just paid the payword (w_4, 4) to vendor V1. Now U needs to pay another vender V2, which U has not done any transactions before, three paywords. What should U send to V2?
   (A) (w_7, 7);
   (B) U needs to check if he/she has (w_7, 7). If yes, U sends (w_7, 7). If no, U needs to generate another payword chain with at least 3 paywords, and send the initial commitment and (w_3, 3);
   (C) U needs to generate another payword chain with at least 3 paywords, and send the initial commitment and (w_3, 3);
   (D) U cannot pay V2, since the broker has not authorized U to do so;
   (E) (w_3, 3).

Answer: _____

2. Consider the MicroMint micro-payment system with parameter k=3. Assume a broker is minting the coins through BINs as described in this protocol. In one of the BINs, there are four values (x1, x2, x3, x4). Which is the following statements is correct?
   (A) The broker can used either (x1, x2, x3) or (x2, x3, x4) as a valid coin;
   (B) The broker can use both (x1, x2, x3) and (x2, x3, x4) as valid coins;
   (C) The broker can use (x1, x2, x3, x4) as a single valid coin;
   (D) The broker cannot use this BIN to generate valide coins;
   (E) None of the above.

Answer: _____

3. Consider the following statements about perfect forward secrecy (PFS):
   (1) It is possible to achieve PFS with a symmetric key as the long term key.
   (2) It is possible to achieve PFS with ephemeral Diffie-Hellman protocol.
   (3) It is possible to achieve PFS with RSA algorithm.
   (4) It is possible to achieve PFS with a symmetric key encrypting the session key.

Which of the following include the set of all correct statements?
(A) 1, 2, 3;
(B) 2;
(C) 1, 2;
(D) 4;
(E) 2, 3.

Answer: _____

4. Which of the following is a correct statement about the cookie mechanism used in the Internet key exchange protocols?

(A) It is a distraction. When an attacker launches attacks against a host, the host gives back some cookies so that the attacker will be distracted by the cookie and stop attacking the victim. The attacker may possibly have a cup of tea while enjoying the cookie, and completely forget the attacks.
(B) The cookie mechanism is a weak authentication mechanism aimed at identifying an attacker's IP address if the attacker launches a resource clogging attack against a victim;
(C) The cookie mechanism can prevent IP spoofing attacks;
(D) Because of the cookie mechanism, all IKE protocols are free of resource clogging attacks.
(E) The cookie mechanism is used to track users' web accesses. It provides a way to keep the state of a user's access over the stateless http protocol.

Answer: _____

5. (20 points) Authentication in IKE can be achieved through pre-shared symmetric keys. However, by doing so the Initiator and the Responder lose the ability to achieve Perfect Forward Secrecy (PFS).

(a) (5 points) Is the above statement correct?

(b) (15 points) If yes, give your justifications. If no, give the protocol steps to achieve PFS with a pre-shared symmetric key and explain why PFS is achieved.

6. (10 points) IKE phase 1 exchanges may work in two modes: main mode and aggressive mode.

(a) (5 points) What are gained by using the aggressive mode instead of the main mode?

(b) (5 points) What are lost by using the aggressive mode instead of the main mode?

7. (15 points) Consider the NetBill system.

(a) (5 points) Can a merchant resubmit an EPO that has been processed by the NetBill server before? (Answer yes or no.)

(b) (10 points) If your answer to (a) is yes, revise the NetBill protocol to prevent this. If your answer is no, explain why this is not possible.

8. (15 points)

(a) (5 points) Alice needs to send a long message to Bob. Assume that all they know about each other is the other party's public key, denoted as PK_A for Alice and PK_B for Bob. Draw a diagram to show how Alice should generate the message to be transmitted if they want to provide source authentication, non-repudiation, and confidentiality of message content. (You will lose 2 points for each mechanism you miss or add unnecessarily.)

(b) (10 points) Suppose Alice needs to send many long messages to Bob during a short period of time. Assume that all they know about each other is the other party's public key, denoted as PK_A for Alice and PK_B for Bob. What should they do to be more efficient than repeating the scenario in (a)? Describe your solution concisely, and then draw diagrams to illustrate your protocol(s). (You will lose 2 points for each mechanism you miss or add unnecessarily.)