CSC650 SECURE NETWORKED SYSTEMS

Spring 2016 Final

Due 7:00PM 2016/5/24

This is a take-home exam. You must work on it independently!

The exam has 11 questions, 10 pages (including this page).

Good Luck ☺

Name: _____

SF ID: _____

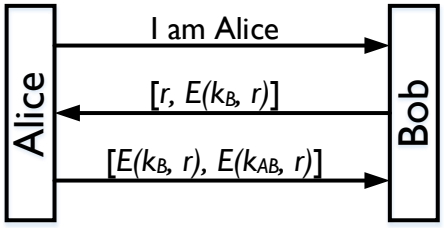
1. (6 Points) Suppose you are doing some online banking using your bank's website. An attacker has set up an active wiretap between your computer and your bank's server. After checking your balance and reading through your transactions, you attempt to log out. However, the attacker uses the active wiretap to send a message requesting to the bank a transfer from your account to an account they control. In the process, this causes your logout message to time out. Describe the ways in which this is an example of attacks on confidentiality, integrity, and/or availability.

2. (10 Points) Suppose Alice has an RSA public key k_A^+ and an RSA private key k_A^-. Bob has an RSA public key k_B^+ and an RSA private key k_B^-. Alice and Bob know each other's public key. Now Alice wants to send a long message m to Bob. How can she protect the message so that, when Bob receives it, he is sure that
   a) Confidentiality: nobody else has viewed the content;
   b) Integrity: no one has modified it;
   c) Non-repudiation: the message is indeed sent from Alice;
   d) Low Computational Complexity: avoid applying the expensive RSA operations on the entire long message m.

   Show what Alice needs to send to Bob and explain how the above four goals are achieved.

3. (10 Points) Design an authentication mechanism for the server Bob to authenticate the user Alice, which can resist both eavesdropping and database reading attacks. Draw the diagram of the scheme and explain why it is secure against eavesdropping and database reading attacks.

4. (5 Points) In HW2, Q8, we show an authentication protocol for the stateless server Bob to authenticate a user Alice, which is not secure. Now let's modify the protocol as follows: Bob is still a stateless server and it sends both a challenge, and the challenge encrypted with a key that only he knows, to Alice. Alice then sends the received encrypted challenge back to Bob, together with the same challenge encrypted with the shared secret key between Alice and Bob.



Is this protocol secure? Explain why or why not.

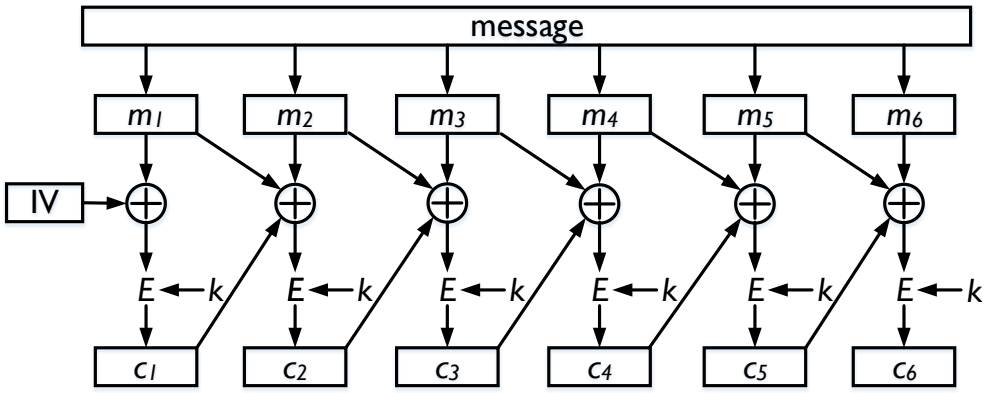
5. (6 Points) What is the drawback of the basic web authentication scheme? How does the digest web authentication scheme overcome it?

6. (10 Points) The following questions refer to Intrusion Detection Systems (IDS).
   a. What is the signature-based IDS? What is the anomaly-based IDS?
   b. IDS may make two kinds of mistakes, i.e., false positives and false negatives. False positive means the IDS believes there is an attack and sends an alert, but no attack occurs in fact. Between signature-based IDS and anomaly-based IDS, which is more likely to incur false positives and why?

7. (5 Points) A network has hosts A, B, C, D, E and F. A and F are connected through B, C, D, and E, i.e., A – B – C – D – E – F. Assuming host A has public keys for all other hosts, describe how it can send a message to host F without letting hosts B, C, D or E know the original sender or ultimate recipient of the message.

8. (8 Points) Describe the SMURF attack and the SYN flooding attack.

9. (15 Points) The following diagram shows the encryption algorithm of a modified version of CBC, which is called Plaintext Cipher Block Chaining (PCBC).



a. Draw the diagram to show the decryption algorithm of PCBC.
b. What is the effect to the decrypted plaintext blocks if a random error happens in one block of ciphertext, say the *i*th ciphertext block c_i?
c. What is the effect to the decrypted plaintext blocks if two ciphertext blocks, e.g., c_i and c_{i+1}, are interchanged during transmission?

10. (20 Points) The following questions refer to IPSec.
    a. Explain what security services ESP, AH, and IKE provide, respectively.
    b. In what kind of circumstances should the tunnel mode or the transport mode be used?
    c. Assume that A and B are communicating with each other and use AH in the transport mode, while firewall F1 and F2 use ESP in the tunnel mode to protect all traffic between them.

       A --- Firewall F1 --- Internet --- Firewall F2 --- B

       Assume A wants to send a TCP packet to B. The structure of the packet is shown below.

       Show the structure of the packet sent out by A, sent out by F1, and received by B, respectively. Also show the source and destination fields (i.e., src and dst) of the IP headers in these packets.
       Hint: When Firewall F1 receives the TCP packet from A, it will keep the AH header and consider it as part of the TCP header.
    d. AH protects the integrity of some fields in the IP header, but not the Time-to-Live (TTL). Why?

11. (5 Points) Describe one attack on computer networks that is not included in the lecture notes.