CS 161 Computer Security
Fall 2005 Joseph/Tygar/Vazirani/Wagner MT 1

PRINT your name: ______________________________, ______________________________
(last) (first)

SIGN your name: ____

PRINT your Unix account name: ___________________________

PRINT your TA's name: ___________________________

You may consult any books, notes, or other paper-based inanimate objects available to you. Calculators and computers are not permitted. Please write your answers in the spaces provided in the test; in particular, we will not grade anything on the back of an exam page unless we are clearly told on the front of the page to look there.

Please be concise.

If you have questions, make a best guess and state your assumptions.

You have 50 minutes. There are 4 questions, of varying credit (100 points total). The questions are of varying difficulty, so avoid spending too long on any one question.

Do not turn this page until your proctor tells you to do so.

Problem 1	
Problem 2	
Problem 3	
Problem 4	
Total	

Problem 1. [Short answer] (30 points)

Give brief answers (one or two sentences) to each of the following.

(a) What is the principle of least privilege? Why is it important?

(b) Is a TCP connection secure against eavesdropping? Why or why not?

(c) You have a copy of Anthony Joseph's certificate chain: his certificate is signed by the EECS department; the EECS department's certificate is signed by UC Berkeley; UC Berkeley's certificate is signed by Verisign. Whose public keys do you need to know in advance in order to obtain the correct public key for Anthony?

Problem 2. [Packet filters] (20 points)

This problem explores some uses and limitations of (stateless) packet filtering firewalls.

You may use the syntax for packet filtering rules from the Sept. 12 lecture. A ruleset is a list of rules, and the first matching rule determines the action taken. A rule is an action followed by a specification of which packets match: e.g., `drop tcp 1.2.3.4:* -> *:25`.

(a) We have an internal webserver, used only for testing purposes, at IP address `5.6.7.8` on our internal corporate network. The packet filter is situated at a chokepoint between our internal network and the rest of the Internet. Can such a packet filter block all attempts by outside hosts to initiate a direct TCP connection to this internal webserver? If yes, show a packet filtering ruleset that provides this functionality; if no, explain why a (stateless) packet filter cannot do it.

(b) Can a packet filter block all incoming email containing the phrase "Make money fast"? If yes, show a packet filtering ruleset that provides this functionality; if no, explain why a (stateless) packet filter cannot do it.

Problem 3. [Source Code Analysis] (20 points)

```
/* Escapes all newlines in the input string, replacing them with "\n". */
/* Requires: p != NULL; p is a valid ’\0’-terminated string */
void escape(char *p) {
    while (*p != ’\0’)
        switch (*p) {
            case ’\n’:
                memcpy(p+2, p+1, strlen(p));
                *p++ = ’\\’; *p++ = ’n’;
                break;
            default:
                p++;
        }
}
```

You may assume that `escape()`’s argument is always non-null and points to a `’\0’`-terminated string.

What’s wrong with this code (from a security point of view)?

Problem 4. [Crypto] (30 points)

Alice wants to send a cellphone text message to Bob securely, over an insecure communication network. Alice's cellphone has a RSA public key K_A and matching private key v_A; likewise, Bob's cellphone has K_B and v_B. Let's design a cryptographic protocol for doing this, assuming both know each other's public keys.

Here is what Alice's cellphone will do to send the text message m:

1. Alice's phone randomly picks a new AES session key k and computes $c = \text{RSA-Encrypt}(K_B, k)$, $c' = \text{AES-CBC-Encrypt}(k, m)$, and $t = \text{RSA-Sign}(v_A, (c, c'))$.
2. Alice's phone sends (c, c', t) to Bob's phone.

And here is what Bob's cellphone will do, upon receiving (c, c', t):

1. Bob's phone checks that t is a valid RSA signature on (c, c') under public key K_A. If not, abort.
2. Bob's phone computes $k' = \text{RSA-Decrypt}(v_B, c)$ and $m' = \text{AES-CBC-Decrypt}(k', c')$.
3. Bob's phone informs Bob that Alice sent message m'.

(a) Does this protocol ensure the confidentiality of Alice's messages? Why or why not?

(b) Does this protocol ensure authentication and data integrity for every text message Bob receives? Why or why not?

(c) Suppose that Bob is Alice's stockbroker. Bob hooks up the output of this protocol to an automatic stock-trading service, so if Alice sends a text message "Sell 100 shares MSFT" using the above protocol, then this trade will be immediately and automatically executed from Alice's account. Suggest one reason why this might be a bad idea from a security point of view.