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. [Firewalls and Network Threats] (30 points)

List and **explain** three network threats that a firewall does not protect against. (If a threat only applies to certain types of firewalls, then explain why this is the case.)

(a) Threat #1

(b) Threat #2

(c) Threat #3

Problem 2. [Zero-Knowledge Proofs] (20 points)

Let (N,e) be Alice's RSA public-key and (N,d) be her private key. Suppose that Bob claims to have a signed message from Alice: he claims to have $s = m^d \bmod N$ for some particular $m \bmod N$ (which he reveals). Bob wishes to prove to Charlie that he has this signed message, without revealing any information about s. The following are the first two steps in a protocol by which Bob can provide a zero-knowledge proof of knowledge about s:

- Bob selects a random number $r \bmod N$ and computes $t = r^e \bmod N$. He sends $t \bmod N$ to Charlie.
- Charlie randomly chooses one of two challenges: I) He asks Bob to send him Alice's signature on t, namely $t^d \bmod N$. II) He asks Bob to send him Alice's signature on $m \cdot t$, namely $(m \cdot t)^d \bmod N$.

1. Fill in the last two steps of the protocol. i.e. how does Bob respond to each challenge. And what should Charlie do to check each response.

2. This protocol is zero knowledge, in the sense that even a cheating verifier gets no information about the original signed message s. Recall that the key step in proving this is showing that there is a simulator who, *without* knowledge of s, can create the transcript of Charlie's interaction with Bob with probability 1/2 regardless of which of the two challenges Charlie issues. Show how the simulator can achieve this goal.

Problem 3. [Firewall Deployments] (20 points)

Explain the strengths and weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, and laptops against network threats.

(a) A firewall at the network perimeter.

(b) Firewalls on every end host machine.

(c) A network perimeter firewall and firewalls on every end host machine.

Problem 4. [Classified Computing] (30 points)

(a) List two examples of covert channels, **other** than the three examples given in the lecture notes: existence of a file, system paging behavior, and system load. Explain how an adversary could take advantage of each of your examples.

- Example #1

- Example #2

(b) Two professors are running applications on a classified multi-user system. Professor Tygar is running the Quake game, and Professor Wagner is running a Top Secret application. Who should get higher priority on a multi-user machine? Explain your answer.

(c) Why is it difficult to implement systems supporting covert channel prevention that perform well? Explain your answer.