CS 161 Computer Security
Fall 2006 Joseph/Tygar

Midterm 2

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

SIGN your name: ____

PRINT your Unix account name: ___________________________

PRINT your TA's name: ___________________________

READ ALL INSTRUCTIONS CAREFULLY.

You are allowed to bring one 8.5"×11" page of handwritten notes with you, but no books, printouts, or other study aids. Calculators, computers, and other electronic devices are not permitted. Please turn off cell phones and music players and keep them off your desk, and remove headphones.

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 explain all work, but be concise.

If you think there is an error or a significant ambiguity in the exam, please bring it to the attention of the exam proctor.

You have 80 minutes. There are four 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. [Covert Channels] (30 points)

(a) (5 points) Write down the Fiat-Shamir zero-knowledge protocol (as presented in class) where Alice proves her identity to Bob with probability 50% each iteration.

(b) (5 points) Identify all the covert channels in the Fiat-Shamir protocol that **Alice** can use to leak information to **Bob**.

(c) (5 points) Identify all the covert channels in the Fiat-Shamir protocol that **Bob** can use to leak information to **Alice**.

(d) (5 points) In view of the above covert channels, in what sense is it fair to call Fiat-Shamir a zero-knowledge protocol — since it leaks information how can it be “zero knowledge”?

(e) (5 points) How do nonces present an opportunity for covert channels?

(f) (5 points) How can we limit leakage of covert channel information via nonces?

Problem 2. [Isolation Techniques] (26 points)

(a) (9 points) Briefly describe the type of isolation used by qmail for security purposes.

(b) (9 points) Briefly explain why the process isolation used by qmail is insufficient from a security point-of-view.

(c) (8 points) Briefly explain what system call interposition is.

Problem 3. [Random Number Generation] (24 points)

(a) (8 points) Bob brilliant has come up with a cryptographically secure pseudorandom bit generator that takes a seed of 128 bits. Show how to turn this into a symmetric cryptosystem with a key of 128 bits.

(b) (8 points) Given a 128-bit seed, what is the maximum number of pseudorandom bits Bob can expect to get from his generator?

(c) (8 points) If a pseudorandom number generator passes statistical tests for randomness, what additional property does it need to be cryptographically secure?

Problem 4. [Firewalls] (20 points)

(a) (10 points) You are given a firewall that can examine the contents of packets, including reconstructing connection streams. What types of buffer overflow attacks can it protect against, if any? What types of buffer overflow attacks can it not protect against, if any? Explain your answers briefly.

(b) (10 points) Explain how you could use such a firewall to protect against transmitting unencrypted credit card numbers over the network.